Crime and Justice in Digital Society 1

Marleen Weulen Kranenbarg
Rutger Leukfeldt *Editors*

Cybercrime in Context

The human factor in victimization, offending, and policing

Springer

Crime and Justice in Digital Society

Series Editors

Anastasia Powell
Royal Melbourne Institute of Technology
Melbourne, VIC, Australia

Murray Lee
University of Sydney
Sydney, NSW, Australia

Travis Linnemann
Eastern Kentucky University
School of Justice Studies
Richmond, KY, USA

Robin Cameron
School of Management
Royal Melbourne Institute of Technology
Melbourne, VIC, Australia

Gregory Stratton
Royal Melbourne Institute of Technology
Melbourne, VIC, Australia

Crime and Justice in Digital Society offers an exciting new platform for theoretical and empirical works addressing the challenges and opportunities of digital society and the Internet of Things for crime, deviance, justice and activism. As digital technologies become progressively embedded into our everyday lives, so too are human-technological interactions embedded into everyday crimes, as well as in cultural representations and justice responses to crime. There is a need for scholarly examination of the ways in which shifts in digital technologies as well as socio-political and socio-cultural structures and practices, are producing and reproducing crime, justice and injustices in contemporary societies. This new book series aims to publish and promote innovative, interdisciplinary, and forward thinking scholarship on crime, deviance, justice and activism in the context of digital societies. Both established and early career scholars are encouraged to submit proposals for research monographs or edited volumes. Crime and Justice in Digital Society is particularly welcoming of research that addresses issues of inequalities and injustices in relation to gender, race, sexuality, ability and/or class, as well as works that push the boundaries of conventional 'cyber' crime studies and engage with interdisciplinary frameworks from across criminology, sociology, studies of technology and society, media and cultural studies, politics, computer sciences and beyond.

More information about this series at http://www.springer.com/series/16101

Marleen Weulen Kranenbarg • Rutger Leukfeldt
Editors

Cybercrime in Context

The human factor in victimization, offending, and policing

Springer

Editors
Marleen Weulen Kranenbarg
Department of Criminal Law
and Criminology
Vrije Universiteit (VU) Amsterdam
Amsterdam, The Netherlands

Rutger Leukfeldt
Netherlands Institute for the Study of Crime
and Law Enforcement (NSCR)
Amsterdam, The Netherlands

Centre of Expertise Cyber Security
The Hague University of Applied Sciences
The Hague, The Netherlands

ISSN 2524-4701 ISSN 2524-471X (electronic)
Crime and Justice in Digital Society
ISBN 978-3-030-60526-1 ISBN 978-3-030-60527-8 (eBook)
https://doi.org/10.1007/978-3-030-60527-8

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2021
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Part I

Introduction

Marleen Weulen Kranenbarg and Rutger Leukfeldt

The second annual conference on the human factor in cybercrime was organized in October 2019 in The Netherlands. During this three day small-scale conference many well-known international researchers presented their latest work on the human factor in cybercrime. The small scale of the conference enabled us to make all sessions plenary. This resulted in lively discussions of the presented research and very useful feedback for the presenters. A large selection of the presented work is included as chapters in this book. This collection of chapters represents the state of the art of research on The Human Factor in Cybercrime. All chapters are based on high quality empirical research and contain a variety of disciplines and theoretical and methodological approaches, all related to human factors in cybercrime.

The goal of this edited volume and the annual conference is to inform academics about these new developments in cutting edge research on the human factor in cybercrime and stimulate future research and collaborations. The next Chapter "The Annual Conference on the Human Factor in Cybercrime: An Analysis of Participation in the 2018 and 2019 Meetings" presents descriptive analyses on the goals and network of participants in the first two editions of the conference. Due to the global COVID-19 pandemic, the third annual conference which was scheduled to be held in Montréal in November 2020 has been postponed until 2021. We are confident that we will continue to strengthen connections in this community and we

M. Weulen Kranenbarg (✉)
Department of Criminal Law and Criminology, Vrije Universiteit (VU) Amsterdam, Amsterdam, The Netherlands
e-mail: m.weulenkranenbarg@vu.nl

R. Leukfeldt
Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam, The Netherlands

Centre of Expertise Cyber Security, The Hague University of Applied Sciences, The Hague, The Netherlands

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

M. Weulen Kranenbarg, R. Leukfeldt (eds.), *Cybercrime in Context*, Crime and Justice in Digital Society I, https://doi.org/10.1007/978-3-030-60527-8_1

hope that the annual conference and its publications such as this book will inspire many new and established researchers in the field.

Similar to the session structure during the conference, the chapters in this book are grouped around three main themes: victims, offenders, and policing. Within these overarching themes, some subthemes can be identified. For victims, the section contains chapters on victim characteristics and behavior, consequences of victimization, and prevention of victimization. For offenders, the section contains chapters on both individuals offenders and their characteristics, and organized groups or communities of offenders. In the section on policing some interesting aspects of policing cybercrime are discussed, such as the context of the TOR-network, problems related to reporting crime to the police and the analysis of crime reports, and potential interventions.

The Annual Conference on the Human Factor in Cybercrime: An Analysis of Participation in the 2018 and 2019 Meetings

Asier Moneva

Introduction

In the land of research, there is a vast forest of academic conferences that grows thicker as we speak. In this forest, many researchers, especially the most inexperienced—and generally the youngest—get lost because they are uncertain which conferences to attend. Generally constrained by limited budgets, researchers must choose a handful of these events at which to disseminate their work and build their networks if they want to have an impact on society. But this forest is so dense that one can easily get lost. Many trails lead to "first and only" events that are crafted with carefully chosen names so broad as to attract a wide range of participants (e.g. the first International Conference on Technology, Knowledge and Human Behaviour).[1] And to accommodate many participants in a short time, large conferences need formulas that allow research to be presented simultaneously. But parallel sessions mean that most research goes unnoticed by many scholars who might find it relevant to their own research. Thus, many researchers end up in these generic events, where the task of effectively exchanging knowledge is overly complex. At these events, disguised as interdisciplinary, participants are likely to have such different agendas that it is difficult for them to find usefulness in each other's research. Amidst all this confusion, which conferences should one attend?

[1] Very possibly there will never be a second edition of such conferences. Note that any resemblance to reality is pure coincidence.

A. Moneva (✉)
Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam, Netherlands

The Hague University of Applied Sciences, The Hague, Netherlands
e-mail: AMoneva@nscr.nl

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

M. Weulen Kranenbarg, R. Leukfeldt (eds.), *Cybercrime in Context*, Crime and Justice in Digital Society I, https://doi.org/10.1007/978-3-030-60527-8_2

Fortunately, there are other formulas that bring together groups of committed active participants who seek to put research into practice. Some groups of scholars and practitioners have tried to address the problem of abstraction by organising small conferences that are focused on particular problems [e.g. the Environmental Criminology and Crime Analysis Symposiums (ECCA) (Wortley & Townsley, 2017)]. Bringing together the most influential actors in the field, these scenarios help raise the level of discussion and advance the discipline (see Bottoms, 2012). The participants of these conferences then become some kind of "soft peer reviewers" who help shape research designs and interpret results within the most stimulating context. In addition, they contribute through criticism to uncover alternative explanations for findings, discuss results and identify directions for future research. Sadly, such conferences are needles in the straw.

In pursuit of the same goals that advance science, the Annual Conference on the Human Factor in Cybercrime was conceived. This chapter provides an overview of the 2018 and 2019 editions of this Conference in order to analyse their strengths and identify what aspects could be improved in order to guide the organisation of the following editions. After introducing a description of the event and its structure in the next section, the chapter presents a series of descriptive analyses that allow understanding aspects such as the Conference attendance, the origin of the participants and the collaboration networks amongst them.

The Annual Conference on the Human Factor in Cybercrime

To learn about the origins of the Annual Conference on the Human Factor in Cybercrime, one needs to go back a few years and understand the development of intellectual movements in the context of growing interest in cybercrime research. One of the pioneering movements in this domain was the International Interdisciplinary Research Consortium on Cybercrime (IIRCC). Formally established in 2015, the IIRCC was conceived as a global initiative that aims to bring together the leading scholars in the field of cybercrime and cybersecurity with practitioners—regardless of their background—to achieve two main objectives: advancing the state of the art in the discipline, and providing solutions for a secure Internet.[2] As prolific researchers, the original proponents of this movement had a great presence at the most important international scientific events, which constituted ideal scenarios to promulgate the principles of the IIRCC. Inspired by this initiative, researchers from all over the world began to join its ranks. According to its website,

[2] It was during an informal gathering at the second Annual Interdisciplinary Conference on Cybercrime—hosted by the Michigan State University, see https://global.broad.msu.edu/events/eventdisplay/20375/the-2nd-annual-interdisciplinary-conference-on-cybercrime—when the participating scholars came up with the idea of providing a formal structure to their meetings, thus originating what is now known as the IIRCC. For more information about the IIRCC, visit: https://cj.msu.edu/iircc/iircc.html.

IIRCC members currently represent institutions from at least that nine different countries. And they continue to thrive.

In parallel, the growing interest in cybercrime research was becoming evident at the two major criminology conferences: The Annual Conference of the European Society of Criminology (EUROCRIM), and the American Society of Criminology (ASC) Annual Meetings. After two decades of history, nobody disputes that these two are the most important criminological research conferences in their respective continents.[3] Over the years, participation in both conferences has continued to grow (Aebi & Kronicz, 2019)[4] along with the presence of cybercrime researchers, setting the tone for news initiatives that transcend territorial boundaries. In response to an increasing volume of cybercrime contributions in both conferences (Fig. 1), a bunch of leading scholars in the field—including many members of the IIRCC—resolved to organise the participation of cybercrime researchers by founding the European Society of Criminology Working Group (ESC WG) on Cybercrime in 2016 and the Division of Cybercrime in 2019. As shown in Table 1, although each has its particularities, both groups preserve the essence of the IIRCC. This is reflected in their mission of bringing together scholars from the field of cybercrime and cybersecurity to exchange knowledge from a global perspective.

Because of its recent creation, the Division of Cybercrime is still in its infancy, but the ESC WG on Cybercrime has been operating for a few years now. To promote the objectives set within the framework of EUROCRIM, one of the fundamental tasks that the chairs of the ESC WG on Cybercrime undertake consists in arranging all cybercrime presentations in such a way that there are no parallel sessions, so that all scholars interested in the topic can attend every presentation. This is no easy task, as to date the working group is composed of 83 researchers, but it certainly favours cybercrime research and also creates a meeting point for cybercrime scholars. However, even if these organisations succeed in this task and manage to improve the cybercrime research scenario in their respective conferences, they would still have to solve other problems in order to achieve their goals. First, the scope of these conferences is—as their name suggest—territorially limited, and to attend such events one must become a member of the societies that organise them by paying a fee (i.e. the ESC or the ASC). Therefore, the very nature of each conference limits the networking capacity of the participants and, with it, the ability to advance the field. And second, EUROCRIM and the ASC Annual Meeting are Criminology conferences that are full of criminologists. This is important because cybercrime research encompasses too wide a field and incorporates many objects of study that are approached from very different theoretical frameworks and methodologies. It is therefore impractical to make an approach from a single discipline. Additionally, this sometimes makes communication between cybercrime researchers difficult.

[3] For more information about the conferences, visit https://www.esc-eurocrim.org/index.php/conferences/upcoming-conferences for EUROCRIM, and https://www.asc41.com/annualmeeting.html for the ASC Annual Meeting.

[4] The historical ASC Annual Meeting attendance figures can be consulted in: https://www.asc41.com/history/Annual%20Meeting%20Misc/ASC_Annual_Meeting_Attendance_Figures.pdf.

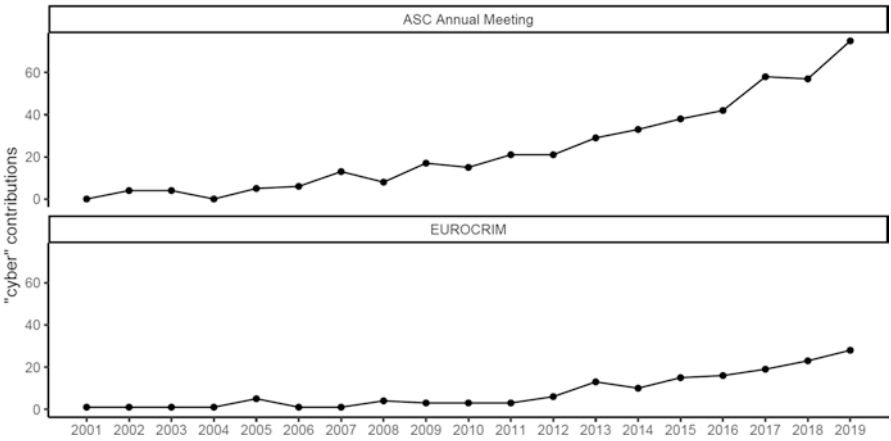

Fig. 1 Number of contributions presented at the ASC Annual Meeting and EUROCRIM with the string "cyber" in the title (Source: ASC Annual Meeting and EUROCRIM final programmes (2001–2019))

Table 1 Objectives of the ESC WG on cybercrime and the Division of Cybercrime

ESC WG on Cybercrime	Division of cybercrime
1. Advancing knowledge and research on cybercrime and cybersecurity across Europe (both substantively and methodologically) and other parts of the world, including the United States, the Middle East, and Asia, with plans to expand to other parts of the world 2. Creating a network for information exchange and international collaboration between leading scholars, starting scholars, graduate students, government agencies, and private organizations involved in cybercrime research	1. To bring together in one multi- and inter-disciplinary division, those actively engaged in research, teaching, and/or practice in the field of cybercrime and cybersecurity 2. To encourage scholarly, scientific, and practical exchange and collaboration concerning cybercrime and cybersecurity within a global perspective 3. To develop effective cybercrime prevention strategies and practices 4. To provide a forum for interaction and the exchanging of ideas among persons involved in cybercrime and cybersecurity 5. To promote conference sessions pertaining to cybercrime and cybersecurity

Source: The ESC WG on Cybercrime website, https://www.cybercrimeworkingroup.com/; and the Constitution of the Division of Cybercrime

To illustrate potential communication problems, note there is a great stretch from the most technical approaches that require knowledge in computer engineering and data science, to the most theoretical approaches that require a deep understanding of phenomena from the social sciences. In a field as young as cybercrime, this divergence allows many research questions to be examined. But in order to achieve greater depth and scientific rigour, it is necessary to deepen certain questions from the standpoint of specialisation. In favour of the latter, scholars promoting a new conference model urged a more specific thematic shift: from *cybercrime* to *the human factor in cybercrime*. The Human Factor in Cybercrime encompasses several aspects: the victims who suffer from it, the offenders who commit it, the police strategies that are implemented for its formal control, the role that people and institutions have in its social control, the interaction between all these actors and the environment for its prevention, and the contribution of criminological theory in understanding and modelling all of them (Leukfeldt, 2017; Leukfeldt & Holt, 2020). The study of all these topics is primarily approached from the lens of the social sciences but needs both interdisciplinarity to thrive and a strong venue for the transfer of knowledge.

To overcome these obstacles, two IIRCC members proposed at the 2017 ASC Annual Meeting in Philadelphia to organise a different conference scheme in 2018. The new conference would not be just continental, but global, and no membership fees would be requested, only the costs incurred by the participation. Participation would be open to any academics who are active in the field and want to present their work among their peers. Submitted abstracts would then be subjected to a peer review process that would keep the conference small in participation and linear in its development (i.e. no parallel sessions). In addition to the panels, sessions would include roundtables that address hot topics, keynotes by stakeholders to identify research needs, and pitch sessions to promote collaboration on upcoming research ideas. Such format would encourage all presentations to be heard and receive input from the audience, thus generating richer discussions that improve the knowledge produced. Furthermore, this simpler structure would facilitate the incorporation of stakeholders into these discussions, so that the research produced can be applied, reach the public, and impact on society. In this way, the conference would help to strengthen the link between academia and practice, to promote international collaboration between scholars in the same field, to provide soft peer review on the scholars' work, and ultimately to provide an environment that focuses on advancing the field. This conference would have one additional peculiarity: it would narrow its thematic scope to the Human Factor in Cybercrime.

As a result of both a new conference format and a thematic shift, the Annual Conference on the Human Factor in Cybercrime was created. After the first edition was held in 2018 in Israel, a second one was held in 2019 in The Netherlands consolidating its presence. The third edition—to be held in 2021 in Canada—is already in preparation, ensuring its continuity.

The Present Study

To better understand the growth and development of the Annual Conference on the Human Factor in Cybercrime, an overview of the participation in its two editions of 2018 and 2019 is provided. Inspired by the work of Bichler and Malm (2008) on the ECCA group, in this chapter descriptive analyses—including network analysis—are conducted to better understand the participation in the conference and its structure. The ultimate goal is to assess its strengths and weaknesses to evaluate whether the conference is directed towards achieving the objectives for which it was intended.

Data

Three main data sources are used in this paper. The first is the data retrieved from the public programme of the conferences and related emails[5]; the second is the information about the members of the ESC WG on Cybercrime and the IIRCC publicly available on their respective websites; and the third are the original participation files maintained by the organisers. The latter had to be used to complement the others because the public programme of the 2019 conference only contained the names of the presenters and not all the co-authors. Note that data pertaining to members of the Division of Cybercrime were not included since they were not yet publicly available due to its still recent creation. In addition, informal conversations with the organisers, and other secondary and external public sources were consulted to complete information on participants (e.g. Google Scholar, personal and institutional websites). The final dataset includes the name of participants, their affiliation, and country where they develop their professional activity, whether they are members of the ESC WG on Cybercrime or members of the IIRCC—the seeds of the Annual Conference on the Human Factor in Cybercrime—whether they are stakeholders or academics, whether they participated in each of the two meetings of the conference, whether they constituted the organising committee, and their network of co-authors in such meetings. Regarding the latter, tidy data required to explore the collaboration network is composed of two separate datasets, one for the participants and their characteristics (i.e. nodes) and another delineating the connections between the nodes (i.e. edges). Note that participation is, therefore, measured by the authorship of the contributions submitted, not by physical attendance.

[5] For the 2018 programme, see https://csrcl.huji.ac.il/event/1st-annual-conference-human-factor-cybercrime-DayI; for the 2019 programme, see https://www.rechten.vu.nl/en/research/organization/research-programmes/empirical-normative-studies/human-factor-cybercrime/index.aspx.

Analytic Strategy

A dual analysis strategy is used in this paper. Firstly, a descriptive analysis of the variation in the volume and composition of participation between the 2018 and 2019 conference editions is carried out. This includes the variation in attendance with respect to the type of participants, the type of institutions, and the number of countries involved.

Secondly, Social Network Analysis (SNA) is conducted to examine the collaborative networks in each of the conference editions. SNA allows to study the individuals that compose a network and the relations that exist between them (Wasserman & Faust, 1994). In this study, the individuals that comprise the network are the participants of the two editions of the conference, and the relationships that exist between them are the collaborations found in the contributions presented at the conference. The collaborations in each network are displayed in the form of cliques (Luce & Perry, 1949), subnetworks of participants that are connected to each other. The cohesion of the network is measured by calculating its density, which indicates the ratio of existing relationships (ER) to possible relationships (PR),

$$\text{Density} = \frac{\text{ER}}{\text{PR}}$$

where PR is calculated depending on the size of the network (n).

$$\text{PR}_n = \frac{n \times (n-1)}{2}$$

So, if all participants collaborated with each other forming a large clique, the density of the network would be 1, whereas individual participation in all cases would produce a density of 0.

Data transformation and data visualisation were executed using the tidyverse R package version 1.3.0 (Wickham et al., 2019), the sf R package version 0.9–3 (Pebesma, 2018), and the igraph R package version 0.8.1 (Csárdi & Nepusz, 2006) in RStudio version 1.2.5042 (RStudio Team, 2019) for the R free software version 3.6.2 (R Core Team, 2020).

Results

The results of the descriptive analysis of participation at the conferences held in 2018 and 2019, and how it varied from one edition to another, are shown in Table 2. To this end, participation was analysed at three levels of aggregation: individual, institutional, and national. In general terms, participation in 2019 multiplied compared to 2018, which reflects in an increase in absolute numbers of each of the parameters in the table. However, the percentages reveal the change in participation

Table 2 Variation in participation records in the two editions of the Annual Conference of the Human Factor in Cybercrime

	Conference edition				Variation	
	2018		2019			
Attendance	*n*	%	*n*	%	*n*	%
Participants	26		79		53	
Organising committee	6	23.1	5	6.3	−1	−16.8
ESC WG on cybercrime	12	46.2	27	34.2	15	−12.0
IIRCC	7	26.9	10	12.7	3	−14.2
Stakeholders	1	3.8	8	10.1	7	6.3
Institutions	14		33		19	
Law enforcement	1	7.1	4	12.1	3	5.0
Research	13	92.9	28	84.8	15	−8.1
Government	0	0.0	1	3.0	1	3.0
Countries	5		10		5	

in relative terms. Thus, even though the number of members of the ESC WG on Cybercrime doubled with respect to 2018, their participation decreased by 12% with respect to the total number of attendees. And a similar effect is observed for IIRCC participants (−14.2%). The number of stakeholders involved increased from 1 to 8, representing a 6.3% increase over total attendance. Note that being a member of the ESC WG on Cybercrime and/or the IIRCC, and being a stakeholder are non-exclusive categories (i.e. stakeholders can also be members of these organisations). At the institutional level, the number of unique entities represented increased by 19. In this case, the variation in the distribution of participation at the institutional level implied a relative increase in the participation of government representatives (3%) and law enforcement agencies (5%) to the detriment of research entities, whether they are universities or research institutes (−8%).

Finally, the number of countries represented increased from 5 to 10. While in 2018 only three continents were represented (i.e. Europe, America and Asia), in 2019 all five continents have some form of representation. However, in both cases most participants came from Western Europe and North America (Fig. 2).

Below, the second part of the analysis serves to graphically illustrate conference networking and to examine it in detail. Figure 3 shows the collaborative networks for the 2018 and 2019 meetings. Three features were used to characterise the participants in the network: the size, to distinguish the organising committee; the colour, to indicate whether the participants belong to the ESC WG on Cybercrime and/or the IIRCC; and the shape, to differentiate whether the participants are stakeholders or not. The existing collaborations in the network are displayed as cliques of two or more nodes, which increased from 7 in 2018 to 24 in 2019. For both conference editions, such collaborations are generally mixed between ESC WG on Cybercrime and/or IIRCC members and non-members. In contrast, stakeholders are rarely involved in collaborations with academics, a circumstance only observed on two occasions at the 2019 meeting. Apparently, the members of the ESC WG on

Fig. 2 Participating countries in the two editions of the Annual Conference of the Human Factor in Cybercrime

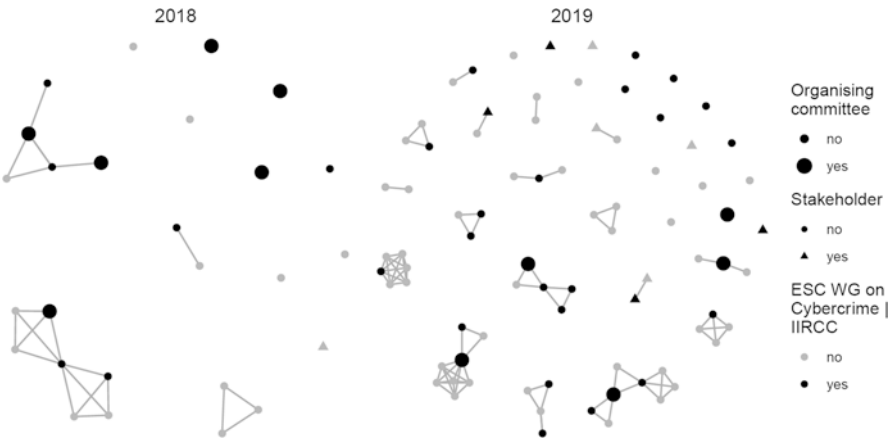

Fig. 3 Collaboration networks in the two editions of the Annual Conference of the Human Factor in Cybercrime

Cybercrime and/or IIRCC play a fundamental role in promoting the cohesion of the network, as they are usually the nexus between various collaborations. Some of them also integrate the organising committee in both editions, which seems more engaged in collaboration in the 2019 meeting. Regarding the cohesion of the network, density analyses yield a value of 0.07 in the 2018 network versus 0.03 in the 2019 network. This means that the ratio of collaborations per participant was higher in the first edition.

Discussion

Although research on the development and purpose of academic conferences is scarce, such an object of study constitutes a cornerstone for the exchange of knowledge that allows for the advancement of scientific disciplines. Research pieces such as Bichler and Malm (2008) on ECCA Symposiums are as infrequent as they are undervalued. In their paper, the authors identify some weaknesses in the social structure of the symposia that allows for their reinforcement in the future. At the very least, the most relevant conferences should consider appointing a commission to conduct this type of research, which serves to evaluate their function and reorient their design. For this reason, we dedicate this chapter to the analysis of the participation in the two Annual Conferences of the Human Factor in Cybercrime held in 2018 and 2019 and the collaboration networks generated within them. Such action allows us to outline some important aspects to be taken into account for the organisation of future editions of the conference.

The first aspect to be highlighted from the conferences is that participation increased considerably in the second edition. One possible explanation is that the success of the first meeting held in Israel increased its popularity among researchers, but it is also likely that the venue for the second meeting (i.e. The Netherlands) was more accessible to participants given their predominant Western background. Such Western dominance has also been observed in similar conferences (Bichler & Malm, 2008). Here it should be noted that participation is mediated by the organising committee. Since its members are responsible for selecting the contributions presented at the conference, it is possible that their preferences bias participation. For example, they may prioritise those contributions in which they collaborate, or they may favour some methodological approaches over others based on their own expertise (e.g. quantitative vs. qualitative). This, in turn, would affect participant diversity. A second relevant aspect to be discussed is the increased presence of stakeholders representing law enforcement agencies and government entities in the conference. Although they still constitute a small percentage of the total number of participants (10.1%), their presence has escalated in the 2019 meeting, even resulting in some joint collaborations with academics. A third aspect to be noted is that the participation of representatives from other countries also increased, bringing a greater diversity of perspectives to the debate due to the more diverse background of the participants (Bichler & Malm, 2008). Together, this resulting expansion is also reflected in the collaborations between scholars, which have increased in total numbers with respect to the first meeting.

Such growth causes the cohesion of the network to decrease in the second meeting, since an arithmetical increase in participation requires a geometric increase in collaborations to maintain the same density. For example, a conference with five participants forming one clique would have a density of 1. If the following year this conference doubled the participation to 10, it would not be enough to also double the collaboration by forming two cliques of five participants, since the potential collaborations would be many more in the second case (i.e. $PR_5 = 10$ compared to

PR_{10} = 45). For this reason, a lower density does not necessarily mean that there is less collaboration among conference participants in the 2019 meeting compared to the 2018 meeting, but rather that it is the result of the growth of the network. Given that the two networks analysed differ greatly in size, it is appropriate to consider network density as an individual measure and not as a comparative one, at least for the time being.

Having assessed the strengths and weaknesses of the conference, a number of recommendations can be listed to help improve its future orientation. Firstly, it appears that the work of the organising committee is bearing fruit by increasing the popularity of the conference in terms of participation and outreach. Future meetings will have to find the balance between size and cohesion so that communication between participants is fluid and encourages both the formation of new collaborations and the enrichment of scientific discussions. A good practice in this regard is the central role assumed by the organising committee in the collaboration networks of the 2019 edition. Upcoming meetings could benefit from the committee's position to cohere the network of participants. Secondly, the participant networks of both editions show that collaboration between researchers and stakeholders is still scarce. Although the involvement of stakeholders is not an objective of the conference, for the research presented to be applied, it is important to encourage the presence of stakeholders that constitute the link between academics and practitioners for two reasons: so that research can be used to solve real problems, and so that strategies to solve such problems are evidence-based. After all, any actors working to mitigate cybercrime and contributing to a better society may benefit from working together. Thirdly, the diversity of participants is essential. Participants from different backgrounds can help the network of academics to identify research needs and provide stakeholders with new perspectives on solving existing problems. Keeping the conference focused on interdisciplinarity would be a step forward in this direction.

However, there are some aspects that were not addressed in this chapter and that—at the same time—pave the way for future research. Note that this chapter only measures collaborations within The Annual Conference on the Human Factor in Cybercrime network, so any other existing collaborations not reflected in the conference programmes were not considered in the analysis. Therefore, it is likely that collaborations between the members of the network are more frequent than what is shown here. Participation of early career researchers was not specifically examined either. Future research should address this issue by devoting special attention to the definition of early career researcher and collecting appropriate data. Generally, it is indispensable that participants' affiliation and membership data are up to date for a rigorous analysis. In this regard, along with continuing to use open data sources, it is advisable to design a specific instrument to collect the data required for evaluating participation in future editions of the conference (i.e. a questionnaire that includes the informed consent of the participants and that complies with current data protection regulations).

Conclusions

This chapter assessed the participation in the two editions of the Annual Conference on the Human Factor in Cybercrime. Two main conclusions can be drawn from the analyses: (1) that the 2019 edition enjoyed a more numerous and varied participation, both in terms of individuals, institutions and countries; and (2) that the members of the ESC WG on Cybercrime and the IIRCC are instrumental in sustaining collaborative networks among participants, despite the fact that there are still many isolated nodes. Overall, it seems that the latest edition of the conference is closer to achieving the objectives for which it was conceived.

Of course, the fact that only two conference meetings were held limits the scope of the recommendations presented in this paper. Nevertheless, with the information available, some structural patterns in participation can be observed that allow useful recommendations to be made. Data from future editions of the conference will allow for more robust analyses that will in turn serve to provide more reliable suggestions.

Acknowledgements To E. Rutger Leukfeldt and Marleen Weulen Kranenbarg for providing the data for the study. To Thomas J. Holt for providing details on the origin of the IIRCC. To Cristina Del-Real for her comments on an earlier draft of this manuscript. To the reviewers, for their insightful comments that helped improve the manuscript. *Funding*: This work was supported by the Spanish Ministry of Science, Innovation and Universities under Grant FPU16/01671, and under Grant EST18/00043.

References

Aebi, M. F., & Kronicz, G. (2019). ESC Executive Secretariat annual report 2018. *Newsletter of the European Society of Criminology, 18*(2), 4–8.

Bichler, G., & Malm, A. E. (2008). A social network analysis of the evolution of the Environmental Criminology and Crime Analysis (ECCA) symposiums. *Crime Patterns and Analysis, 1*, 5–22.

Bottoms, A. (2012). Developing socio-spatial criminology. In M. Maguire, R. Morgan, & R. Reiner (Eds.), *The Oxford handbook of criminology* (pp. 450–489). Oxford: Oxford University Press. https://doi.org/10.1093/he/9780199590278.003.0016

Csárdi, G., & Nepusz, T. (2006). The igraph software package for complex network research. *InterJournal, Complex Systems, 1695*(5), 1–9.

Leukfeldt, E. R. (Ed.). (2017). *The human factor in cybercrime and cybersecurity*. The Hague: Eleven International Publishing. Retrieved from https://www.elevenpub.com/criminology/catalogus/research-agenda-the-human-factor-in-cybercrime-and-cybersecurity-1

Leukfeldt, E. R., & Holt, T. J. (Eds.). (2020). *The human factor of cybercrime*. Abingdon: Routledge.

Luce, R. D., & Perry, A. D. (1949). A method of matrix analysis of group structure. *Psychometrika, 14*(2), 95–116. https://doi.org/10.1007/BF02289146

Pebesma, E. (2018). Simple features for R: Standardized support for spatial vector data. *The R Journal, 10*(1), 439. https://doi.org/10.32614/RJ-2018-009

R Core Team. (2020). *R: A language and environment for statistical computing (version 4.0.0) [Computer software]*. Vienna: R Core Team. Retrieved from https://www.R-project.org/

RStudio Team. (2019). *RStudio: Integrated development environment for R (Version 1.2.5) [Computer software]*. Vienna: RStudio Team. Retrieved from http://www.rstudio.com/

Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge: Cambridge University Press.

Wickham, H., Averick, M., Bryan, J., Chang, W., McGowan, L., François, R., … Yutani, H. (2019). Welcome to the Tidyverse. *Journal of Open Source Software, 4*(43), 1686. https://doi.org/10.21105/joss.01686

Wortley, R., & Townsley, M. (Eds.). (2017). *Environmental criminology and crime analysis* (2nd ed.). Taylor & Francis Group: Routledge.

Part II
Victims

The Online Behaviour and Victimization Study: The Development of an Experimental Research Instrument for Measuring and Explaining Online Behaviour and Cybercrime Victimization

M. Susanne van 't Hoff-de Goede, E. Rutger Leukfeldt, Rick van der Kleij, and Steve G. A. van de Weijer

Introduction

Cybercrime is common and its impact can be significant for victims (Cross, Richards, & Smith, 2016; Jansen & Leukfeldt, 2018; Leukfeldt, Notté, & Malsch, 2019). Cybersecurity professionals have tried to reduce victimization with technical measures such as anti-virus scanners and firewalls. However, these measures often have only a limited effect and much victimization can be traced back to human behaviour (Jansen, 2018; Leukfeldt, 2017). For example, internet users may fill in information on a phishing[1] website when they should not, thereby allowing

[1] Phishing is a form of an online scam, in which criminals copy the emails or websites of legitimate organisations to mislead victims in order to obtain login details and gain access to online accounts.

M. S. van 't Hoff-de Goede (✉)
Centre of Expertise Cyber Security, The Hague University of Applied Sciences, The Hague, The Netherlands
e-mail: m.s.vanthoff-degoede@hhs.nl

E. R. Leukfeldt
Centre of Expertise Cyber Security, The Hague University of Applied Sciences, The Hague, The Netherlands

Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam, The Netherlands

R. van der Kleij
Centre of Expertise Cyber Security, The Hague University of Applied Sciences, The Hague, The Netherlands

The Netherlands Organisation for Applied Scientific Research (TNO), The Hague, The Netherlands

S. G. A. van de Weijer
Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam, The Netherlands

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

M. Weulen Kranenbarg, R. Leukfeldt (eds.), *Cybercrime in Context*, Crime and Justice in Digital Society I, https://doi.org/10.1007/978-3-030-60527-8_3

criminals to misuse that information. Therefore, research into internet users is essential to reduce victimization (Leukfeldt, 2017; Rhee, Kim, & Ryu, 2009; Talib, Clarke, & Furnell, 2010).

If we want to prevent cybercrime victimization, we must first explain victimization. Previous cybercrime victimization studies have focused on establishing a risk profile for victims and have attempted to identify factors that could increase the risk of victimization. In these studies, personal characteristics and routine activities are often central, for example, by assuming that certain routine activities, such as using social media, make potential victims more visible to cybercriminals. However, taking the studies together, it does not seem possible to establish an unambiguous risk profile (Bossler & Holt, 2009, 2010; Holt & Bossler, 2013; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010; Van de Weijer & Leukfeldt, 2017). Cybercriminals are apparently not too picky and do not select whom they attack: Everyone is a potential victim of cybercrime. Moreover, it appears that certain online activities are only related to the risk of victimization of specific forms of cybercrime. There do not seem to be any routine activities that are by definition risk-increasing (Leukfeldt & Yar, 2016). It is thus not possible to outline a profile of high-risk personal characteristics or routine activities for cybercrime victimization (Leukfeldt, 2014).

The current study focuses on the behaviour of internet users in explaining online victimization. It has been widely recognized that humans are the "weakest link" in cybersecurity. Unsafe online behaviour, such as using weak passwords and not updating software regularly, may increase the risk of cybercrime victimization (Leukfeldt, 2014; Shillair et al., 2015). However, knowledge about how citizens defend themselves against cybercrime is scarce (for an overview, see, for example, Leukfeldt, 2017). It is still unknown how well internet users protect themselves against cybercrime, partly because how people *say* or *think* they behave online is not always the same as how people *actually* behave online (Crossler et al., 2013; Debatin, Lovejoy, Horn, & Hughes, 2009; Workman, Bommer, & Straub, 2008). However, such knowledge is indispensable for the empirical foundation of possible behavioural interventions. It is therefore necessary to gain more insight into the way internet users actually behave online and which factors are associated with this.

This chapter will outline the development of the research tool for the online behaviour and victimization study that can measure actual online behaviour along with possible explanatory factors. The added value of this research instrument is evident: we go beyond existing studies that are often based on self-report by measuring both perceived and actual behaviour among a large-scale sample. Moreover, we do aim to explain not only victimization of specific forms of cybercrimes, but also several clusters of online behaviour. After all, there are many types of behaviour that increase the risk of certain cybercrimes. In addition, simultaneously, it does not have to be the case that a certain behaviour always leads to a certain form of victimization. On one occasion, falling for a phishing email can lead to an empty

bank account, while on another, it can lead to a ransomware[2] infection or be the start of a spear phishing[3] attack on the company where the victim works (see, for example, Leukfeldt, Kleemans, & Stol, 2017; Lusthaus, 2018). Therefore, the research instrument presented in this chapter objectively measures a number of behaviours that we know to be directly related to the victimization of various cybercrimes, such as sharing personal information and using weak passwords. Furthermore, this research instrument is innovative because it measures various explanations for online behaviour and victimization, while existing studies often only examine attitudes or awareness Finally, the tool includes several experiments to determine, for example, whether persuasion techniques used by criminals make individuals more likely to engage in unsafe online behaviour.

Online Behaviour and Cybercrime Victimization

Unsafe Online Behaviour as a Predictor of Online Victimization

Unsafe online behaviour can directly contribute to increased risk of victimization. Victims of online banking fraud, for example, often appear to have inadvertently given their personal information to fraudsters, for example by clicking on a hyperlink in a phishing email or entering information on a phishing website (Jansen, 2018; Jansen & Leukfeldt, 2015, 2016).

An important condition for online safety is therefore safe online behaviour (i.e. cyber hygiene behaviour, Cain, Edwards, & Still, 2018). People who behave safely online—or cyber hygienically—adhere to "golden" rules (best practices). For example, they avoid unsafe websites, prevent clicking on unreliable hyperlinks, use strong passwords and keep their technical security measures up to date (Cain et al., 2018; Crossler, Bélanger, & Ormond, 2017; Symantec, 2018). Based on previous empirical studies, we identified seven central behavioural clusters for this study: password management, backing up important files, installing updates, using security software, being alert online, online disclosure of personal information and handling attachments and hyperlinks in emails. When internet users display safe behaviour within each cluster, this may protect them from cybercrime victimization (for more information, see Cain et al., 2018; Crossler et al., 2017; Van Schaik et al., 2017).

Previous studies, based on both self-reported behaviour and actual behaviour in experimental settings, have shown that many people only behave safely online to a limited degree or even display patently unsafe online behaviour, on each of the

[2] Ransomware is a malicious software that blocks a computer or encrypts files. Only when you pay a ransom you are able to use the computer or files again.

[3] Spear phishing is a targeted phishing attack against a person or a specific group of people.

seven behavioural clusters. Many people do not have a malware[4] scanner or firewall on their home computer, or do not keep them up to date (Cain et al., 2018; Van Schaik et al., 2017). In addition, young people are lax with their smartphone security (Jones & Heinrichs, 2012; Tan & Aguilar, 2012). While the use of unique strong passwords is an important security measure, studies have shown that 50–60% of passwords are reused across platforms, and that many people would share their passwords with others (Alohali, Clarke, Li, & Furnell, 2018; Cain et al., 2018; Kaye, 2011). Another example of unsafe online behaviour is that people share personal information on social media on a large scale (Christofides, Muise, & Desmarais, 2012; Debatin et al., 2009; Talib et al., 2010), which can be used to make phishing emails more credible (spear phishing) or to commit identity fraud. For example, many of the respondents in the study by Talib et al. (2010) shared their full name and email address (62%), date of birth (45%), or full address (7%) on an online social network. Finally, online deviant behaviours, such as illegal downloading, online bullying and threatening others, are common and contribute to online victimization, possibly especially among young people (Bossler & Holt, 2009; Holt & Bossler, 2013; Maimon & Louderback, 2019; Ngo & Paternoster, 2011).

A further conclusion that can be drawn from the literature is the added value of focusing on behaviour rather than on specific cybercrimes. Hacking victimization, for example, can be caused by many different behaviours. For example, people can be hacked because they have shared personal information, downloaded malware, or do not have up-to-date security. Moreover, these behaviours can also lead to victimization of other forms of cybercrime, such as online fraud or identity fraud. Studies that focus on specific crimes only provide insight into a small part of the complexity of online behaviour and cybercrime. By focusing on online behaviour, on the other hand, a wide range of cybercrimes can potentially be tackled.

Explaining Online Behaviour

Although safe online behaviour may be of great importance to prevent cybercrime victimization, unsafe online behaviour is common. How can this be explained? Based on two theories that have previously been used to explain behaviour, Protection Motivation Theory (PMT) (Floyd, Prentice-Dunn, & Rogers, 2000; Norman, Boer, & Seydel, 2005) and the COM-B framework (Capability, Opportunity, Motivation, Behaviour) (Michie, Van Stralen, & West, 2011), several constructs can be distinguished that each may play a role in unsafe online behaviour. These are motivation for safe online behaviour, knowledge about safe online behaviour (i.e. awareness) and opportunity for safe online behaviour. After discussing these factors and previous studies on their relationships with online behaviour, this chapter will also focus on other potentially relevant factors.

[4] Malware is malicious software that is installed on your computer unsolicited and usually unnoticed. Examples of malware are viruses, Trojan horses, worms, and spyware.

Motivation

According to PMT, how well we protect ourselves is influenced by the degree to which we are motivated to protect ourselves (Floyd et al., 2000; Norman et al., 2005). People with high protection motivation supposedly act more cautiously and take measures to protect their safety (Crossler & Bélanger, 2014; Floyd et al., 2000). It is argued in PMT that protection motivation is influenced by coping appraisal and threat appraisal; a persons' evaluation of the threat and the measures against this threat (Floyd et al., 2000). Both threat appraisal and coping appraisal have several components. The components of threat appraisal are perceived vulnerability (assessment of one's own vulnerability to the threat) and perceived severity (assessment of the severity of the threat). Coping appraisal includes the components response-efficacy (whether a measure will be effective against the threat), self-effectiveness (whether he/she is able to implement an effective measure) and response costs (whether the estimated costs of taking measures are worth it).

PMT has previously been applied to online behaviour. Previous studies found that estimated response-efficacy, self-efficacy and response costs seem to be important predictors of safe online behaviour (Arachchilage & Love, 2014; Crossler et al., 2017; Crossler & Bélanger, 2014; Jansen & van Schaik, 2017; Rhee et al., 2009; Van Schaik et al., 2017; Workman et al., 2008). However, perceived vulnerability may not be related to safe online behaviour in the expected manner. People who consider themselves vulnerable to online attacks do not behave differently (Jansen, 2018) and may even behave less safely (Crossler & Bélanger, 2014). Related to perceived vulnerability, Boss, Galletta, Lowry, Moody, and Polak (2015) found that fear of victimization did not seem to affect the intention of computer users to back up their files, while it did seemed to increase their intention to use anti-malware software. Finally, most studies find a relationship between perceived severity and online behaviour (Crossler et al., 2017; Jansen, 2018; Jansen & van Schaik, 2017). However, Downs, Holbrook, and Cranor (2007) did not find the estimated severity of the consequences of a successful phishing attack to be a predictor for precautionary behaviour in their sample of 232 computer users.

Unfortunately, very few studies have gone beyond studying protection motivation and attitudes to measure online behaviour. The few that did mainly focused on self-reported precautionary behaviour. It remains unclear how motivation may be related to actual online behaviour.

Knowledge/Awareness

The theoretical COM-B framework (Michie et al., 2011) suggests that in addition to motivation, a necessity for safe online behaviour is capacity (i.e. knowledge about online safety), also referred to as awareness. Examples are knowledge about online threats, information security, safety measures and being able to recognize malicious URLs.