Tennessee TECH

OAK RIDGE National Laboratory

Proceedings of the 16th International Conference on Cyber Warfare and Security

Tennessee Tech University and Oak Ridge National Laboratory
Cooksville, Tenessee, USA
25-26 February 2021

Dr. Juan Lopez Jr., Dr. Ambareen Siraj and Dr. Kalyan Perumalla

aci

A conference managed by ACI, UK

Proceedings of the

16th International Conference on Cyber Warfare and Security ICCWS 2021

A Virtual Conference Hosted By

Tennessee Tech University and the Oak Ridge National Laboratory USA

25-26 February 2021

Copyright the authors, 2021. All Rights Reserved.

No reproduction, copy or transmission may be made without written permission from the individual authors.

Review Process
Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy
ACIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:
http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academic-conferences-and-publishing-international-limited/

Self-Archiving and Paper Repositories
We actively encourage authors of papers in ACIL conference proceedings and journals to upload their published papers to university repositories and research bodies such as ResearchGate and Academic.edu. Full reference to the original publication should be provided.

Conference Proceedings
The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

The Electronic version of the Conference Proceedings is available to download from DROPBOX https://tinyurl.com/ICCWS21 Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.

The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-912764-88-4
E-Book ISSN: 2048-9889
Book version ISBN: 978-1-912764-87-7
Book Version ISSN: 2048-9870
Published by Academic Conferences International Limited
Reading, UK
+44-118 324 6938
www.academic-conferences.org
info@academic-conferences.org

Contents

Preface

These proceedings represent the work of contributors to the 16th International Conference on Cyber Warfare and Security (ICCWS 2021), hosted by joint collaboration of Tennessee Tech Cybersecurity Education, Research and Outreach Center (CEROC), Computer Science department and the Oak Ridge National Laboratory, Tennessee on 25-26 February 2021. The Conference Co-Chairs are Dr. Juan Lopez Jr, Oak Ridge National Laboratory, Tennessee, and Dr. Ambareen Siraj, Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC), and the Program Chair is Dr. Kalyan Perumalla, from Oak Ridge National Laboratory, Tennessee.

ICCWS is a well-established event on the academic research calendar and now in its 16th year, the key aim remains the opportunity for participants to share ideas and meet the people who hold them. The conference was due to be held at Tennessee Tech University, Cookeville Tennessee, but due to the global Covid-19 pandemic it was moved online to be held as a virtual event. The scope of papers will ensure an interesting two days. The subjects covered illustrate the wide range of topics that fall into this important and ever-growing area of research.

The opening keynote presentation is given by Dr. Deborah Frincke, Associate Laboratory Director for National Security Sciences at Oak Ridge National Laboratory, USA, on the topic of *"What's Science Got to Do With it?".* The second day of the conference will open with an address by Ms. Diane M. Janosek, Deputy Commandant for the National Cryptologic School, NSA on the topic of *Cyber Partnerships for the Future.*

With an initial submission of 140 abstracts, after the double blind, peer review process there are 47 Academic research papers, 2 PhD research papers, 6 Masters Research papers, 2 Non-Academic papers and 4 work-in-progress papers published in these Conference Proceedings. These papers represent research from Australia, Austria, Brazil, Croatia, Estonia, Finland, France, Germany, Ireland, Morocco, Romania, Russia, South Africa, UK, and the USA.

We hope you enjoy the conference.

Dr. Juan Lopez Jr., Dr Kalyan Perumalla and Dr. Ambareen Siraj
Oak Ridge National Laboratory and Tennesse Tech University,
Tennessee
USA
February 2021

ICCWS Conference Committee

Dr. Kareem Kamal A.Ghany, Beni-Suef University,, Egypt; Prof Azween Abdullah, Taylors University, Malaysia; Dr William ("Joe") Adams, Univ of Michigan/Merit Network, USA; Assc Ali Al Mazari, ALFAISAL University PS-CoB, Saudi Arabia; Prof Hamid Alasadi, Iraq University college, Iraq; Dr Elie Alhajjar, USMA, USA; Prof. Todd Andel, University of South Alabama , USA; Prof. Antonios Andreatos, Hellenic Air Force Academy, Greece; Dr. Leigh Armistead, Edith Cowan University, Australia; Leigh Armistead, Oak Ridge National Laboratory, USA; Researcher Jawad Awan, Institute of Information & Communication Technology, Pakistan; Mrs Stacey Baror, University of Pretoria, South Africa; Prof. Richard Baskerville, Georgia State University, USA; Dr Zakariya Belkhamza, Ahmed Bin Mohammed Military College, Qatar; Dr. Noam Ben-Asher, IBM/US Army Research Lab, USA; Prof Vijay Bhuse, Grand Valley State University, USA; Prof. Alexander Bligh, Ariel University Center, Ariel, Israel; Dr. Svet Braynov, University of Illinois, Springfield, USA; Dr. Raymond Buettner, Naval Postgraduate School, USA; Dr. Acma Bulent, Anadolu University, Eskisehir, Turkey; Ivan Burke, CSIR, Pretoria, South Africa; Dr Mustafa Canan, Naval Postgraduate School, USA; Dr. Jim Chen, U.S. National Defense University, USA; Mr Ben-Douglas Christie, , UK; Prof. Sam Chung, University of Washington, Tacoma, USA; Dr. Nathan Clarke, University of Plymouth, UK; Dr. Ronen Cohen, Ariel University Centre, Israel; Mr Edwin Covert, WarnerMedia, USA; Dr Paul Crocker, University of Beira Interior, Portugal; Dr. Michael Dahan, Sapir College, Israel; Geoffrey Darnton, Requirements Analytics, UK; Dr. Dipankar Dasgupta, University of Memphis, USA; Evan Dembskey, UNISA, South Africa; Dorothy Denning, Naval Post Graduate School, USA; Dr. Glenn Dietrich, University of Texas, Antonio, USA; Prokopios Drogkaris, University of the Aegean, Greece; Prof. Mariki Eloff, University of South Africa, South Africa; Prof. Eric Filiol, ENSIBS, Vannes, France & CNAM, Paris, France; Larry Fleurantin, Fleurantin, Francois & Antonin, P.A., North Miami Beach, USA; Dr Noluxolo Gcaza, Tshwane University of Technology, South Africa; Dr. Ahmad Ghafarian, University of North Georgia, USA; Dr Scott Graham, Air Force Institute of Technology, USA; Prof. Dr. Tim Grant, Retired But Active Researcher, The Netherlands; Dr John Gray, Nova Southeastern University, USA; Virginia Greiman, Boston University, USA; Dr. Michael Grimaila, Air Force Institute of Technology, USA; Daniel Grosu, Wayne State University, Detroit, USA, USA; Dr. Per Gustavsson, Combitech / Swedish Defence University / George Mason Univeristy, Sweden; Dr Ulrike Hugl, University of Innsbruck, Austria; Dr. John Hurley, National Defense University, USA; Prof. Bill Hutchinson, Edith Cowan University, Australia; Dr. Berg Hyacinthe, State University of Haiti, Haiti; Prof. Barry Irwin, Noroff, Oslo, Norway; Ramkumar Jaganathan, VLB Janakiammal College of Arts and Science (affiliated to Bharathiar University), India; Prof. Leonard Kabeya Mukeba Yakasham, ESURS/ISTA-KIN & ASEAD, DR Congo; Dr Ezhil Kalaimannan, University of West Florida, USA; Dr Bilge Karabacak, Freelance, USA; Dr Saltuk Karahan, Old Dominion University, USA; ; Prof Jesuk Ko, Universidad Mayor de San Andres, Bolivia; Dr Anne Kohnke, Lawrence Technological University, USA; Dr Ahmet Koltuksuz, Yasar University, Turkey; Dr Maximiliano Korstanje, University of Palermo, Buenos Aires, Argentina, Argentina; Michael Kraft, CSC, USA; Prashant Krishnamurthy, University of Pittsburgh, USA; Prof. Hennie Kruger, North-West University, South Africa; Mr. Peter Kunz, DoctorBox, Germany; Rauno Kuusisto, Finnish Defence Force, Finland; Dr Gregory Laidlaw, University of Detroit Mercy, USA; Dr Arash Lashkari, UNB, Canada; Dr Sylvain (Sly) Leblanc, Royal Military College of Canada, Canada; Louise Leenen, CSIR, Pretoria, South Africa; Prof Martti Lehto, University of Jyväskylä, Finland; Dr Antoine Lemay, École Polytechnique de Montréal, Canada; Dr. Andrew Liaropoulos, University of Piraeus, Greece; Mr Trupil Limbasiya, NIIT University, Neemrana, Rajasthan,India; Juan Lopez, Oak Ridge National Laboratory,USA; Volodymyr Lysenko, University of Washington, USA; Dr. Bill Mahoney, University of Nebraska, Omaha, USA; Dr Naufal Mansor, Kampus Uniciti Alam,, Malaysia; Dr Naufal Mansor, Kampus Uniciti Alam,, Malaysia; ASSI Haribabu Maruturi, qiscet, india; Dr Paul Maxwell, Army Cyber Institute, USA; Dr. Todd McDonald, Air Force Institute of Technology, USA; Dr. Robert Mills, Air Force Institute of Technology, USA; Dr Pardis Moslemzadeh tehrani, University of Malaya, malaysia; Dr. Barry Mullins, Air Force Institute of Technology, USA; Prof Antonio Muñoz, University of Málaga, Spain; Dr. Lilian Nassif, Public Ministry of Minas Gerais, Brazil; Dr Asoke Nath, St. Xavier's College(Autonomous), India; Daniel Ng, C-PISA/HTCIA, China; Dr Emmanuel OGU, Babcock University, Ilishan-Remo, Ogun State., Nigeria; Dr. Funminiyi Olajide, Nottingham Trent University, UK; Mr Arif Mohamed Ismail Oliullah, Jefferies International Lts, UK; Prof. Abdelnaser Omran, School of Economics, Finance and Banking, Universiti Utara Malaysia, Malaysia; Prof. Dr. Frank Ortmeier, Otto-von-Guericke Universität, Magdeburg, Germany; Rain Ottis , Tallinn University of Technology, Estonia; Prof. Evgeny Pashentsev, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, Russia; Prof. Graham Payne, Old Dominion University, Virginia, USA; Kalyan Perumalla, Oak Ridge National Laboratory, USA; Dr. Gilbert Peterson, , USA; Pete Peterson, Ministry of Foreign Affairs of the Russian Federation, USA; Rodney Peterson, NIST, US Gov , USA; Andy Pettigrew, George Washington University, USA; Dr. Jackie Phahlamohlaka, Council for Scientific and Industrial Research, Petoria, South Africa; Ms Heloise Pieterse, CSIR, South Africa; Dr Bernardi Pranggono, Sheffield Hallam University, UK; Prof Carlos Rabadão, Politechnic of Leiria, Portugal; Dr Trishana Ramluckan, University of KwaZulu-Nata, South Africa; Prof. Aunshul Rege, Temple University, USA; Dr. Ken Revett, British University, Egypt; Lieutenant Colonel Ernest Robinson, U.S. Marine Corps / Air War College, USA; Dr. Neil Rowe, US Naval Postgraduate School, Monterey, USA; Prof. Lili Saghafi, Canadian International College, Montreal, Canada; Dr Char Sample, US Army Research Laboratory, USA; Ramanamurthy Saripalli, Pragati Engineering College, India; Dr. Mark Scanlon, University College Dublin, Ireland; Corey Schou, Idaho State University, USA; Dr. Yilun Shang, Singapore University of Technology and Design, Singapore; Dr. Dan Shoemaker, Centre for Assurance Studies, USA; Prof. Ma Shuangge, Yale University, USA; Mr. Paul Simon, Air Force Institute of Technology, USA; Ambareen Siraj, ,; Dr. Elena Sitnikova, University of South Australia, Australia; Prof. Aelita Skarzauskiene, Mykolas Romeris University, Lithuania; Ass. Prof. Dr. Risby Sohaimi, National Defence University of Malaysia, Malaysia; Dr. Joseph Spring, University of Hertfordshire, UK; Dr. William Spring, University of Hertfordshire, UK; Dr. Kevin Streff, Dakota State University, USA; Dennis Strouble, Air Force Institute of Technology, USA; Dr. Arwin Sumari, State Polytechnic of Malang, Java, Indonesia; Dr Hamed Taherdoost, Research Club, Research and Development Department of Hamta Group, Hamta

Business Solution, Malaysia; Mr. Unal Tatar, University at Albany - SUNY, USA; Pardis Moslemzadeh Tehrani, University of Malaya,; Peter Thermos, Columbia Univeristy/Palindrome Technologies, USA; Dr. Bhavani Thuraisingham, University of Texas at Dallas, USA; Dr. Socaciu Tiberiu, University of Suceava, Romania; Mr. Patrick Tobin, University College Dublin, Ireland; Dr Antonio Jorge Tomeu-Hardasmal, University of Cadiz, Spain; Dr Hong-Ngoc Tran, University College Dublin, Ireland; Dr Eric Trias, Air Force Institute of Technology, USA; Dr. Chia-Wen Tsai, Ming Chuan University, Taiwan; Brett van Niekerk, University of KwaZulu-Natal, South Africa; Dr Namosha Veerasamy, Council for Scientific and Industrial Research, South Africa; Stylianos Vidalis, School of Computer Science, University of Hertfordshire, UK; Prof. Kumar Vijaya, High Court of Andhra Pradesh, India; Dr. Natarajan Vijayarangan, Tata Consultancy Services Ltd, India; Dr Khan Ferdous Wahid, Airbus Group, Germany; Prof. Murdoch Watney, University of Johannesburg, South Africa; Richard Wilson, Towson University, USA; Hongyi Wu, Old Dominion University, Virginia, USA; Enes Yurtoglu, Turkish Air War College, Turkey; Dr. Zehai Zhou, University of Houston-Downtown, USA

Biographies

Conference and Programme Chairs

Dr. Juan Lopez Jr., USMC (ret) is a cyber-physical R&D program manager at Oak Ridge National Laboratory located in Oak Ridge, TN. He leads research in Critical Infrastructure Protection, Supervisory Control and Data Acquisition (SCADA) systems, Nuclear Power Cybersecurity, and Electromagnetic Interference (EMI) modeling. He served as the technical lead in SCADA/ICS research at the Air Force Cyberspace Technical Center of Excellence located at the Air Force Institute of Technology on Wright-Patterson AFB, OH. Dr. Lopez earned a Ph.D. in Computer Science at the Air Force Institute of Technology, Bachelor of Science from the University of Maryland, Master of Science from Capitol College, and Master of Science from the Air Force Institute of Technology under the NSA's Information Assurance Scholarship Program. Dr. Lopez is an IEEE Senior Member, Co-Chair for the Industrial Society of Automation's Work Group 4, Task Group 7 (Security of ICS Sensors), Certified Information Systems Security Professional (CISSP), Certified SCADA Security Architect (CSSA), Certified Scrum Master, Lean Six Sigma Green Belt, and has an Extra Class amateur radio license from the Federal Communication Commission (FCC).

Dr. Ambareen Siraj is a professor of Computer Science and the founding director of Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC). She has served as the leader on several NSF and NSA education and workforce development grants. Siraj is also the founder of the Women in CyberSecurity (WiCyS) organization, an initiative to recruit, retain and advance women in cybersecurity. Her efforts to educate students and enhance the cybersecurity field of study goes beyond classes, research, outreach projects, workshops and conferences. Dr. Siraj's research focus is on security in cyber-physical systems, Internet of Things, situation assessment in network security, security education and workforce development. She has authored or co-authored more than 50 publications. She is a frequent speaker in various cybersecurity conferences on topics ranging from education, curriculum, workforce development, outreach, security issues & solutions for cyber-physical systems to diversity and inclusion in cybersecurity. Dr. Siraj is recipient of the Colloquium for Information Systems Security Education Exceptional Leadership in Education Award in 2018.

Dr. Kalyan Perumalla is a Manager and Distinguished Scientist at the Oak Ridge National Laboratory. He founded and currently leads the Discrete Computing Systems Group in the Computer Science and Mathematics Division at ORNL. He also serves as an Adjunct Professor at the Georgia Institute of Technology and as a Joint Full Professor in Industrial Engineering at the University of Tennessee. He was a Fellow of the Institute of Advanced Study at Durham University, UK, and a member of the National Academy of Sciences' Technical Advisory Boards for the U.S. Army Research Laboratory. Dr. Perumalla is among the first recipients of the U.S. Department of Energy Early Career Award in high-performance computing. Over the past 20 years, he has served as a principal investigator (PI) or co-PI on several research projects sponsored by government agencies including the Department of Energy, Department of Homeland Security, Air Force, DARPA, Army Research Laboratory, National Science Foundation, and industry.

Keynote Speakers

Dr Deborah Frincke is the Associate Laboratory Director for National Security Sciences at Oak Ridge National Laboratory who guides the research and development of science-based solutions to complex threats. She recently was appointed as the U.S. representative to the NATO Emerging and Disruptive Technologies Advisory Board and was named a Fellow of ACM, the world's largest association of computing professionals. Deborah joined ORNL from the National Security Agency (NSA), where she served in three roles between 2011 and 2020. Her most recent role (until early 2020) was as the Director of the Research Directorate at NSA, where she led the largest in-house research organization in the U.S. Intelligence Community. She was also a founding member of the NSA Board of Directors and the first NSA Innovation Champion. Prior to joining NSA, she had a threefold career encompassing academia, reaching the rank of full professor at University of Idaho; serving as Chief Scientist for Cybersecurity at Pacific Northwest National Laboratory; and launching a successful cybersecurity startup company, TriGeo Network Systems. She has published approximately 200 articles and technical reports.

Diane M. Janosek is an award-winning cybersecurity leader and sought-after speaker. As an innovator, she has been a member of the Defense Intelligence Senior Executive Service (SES) since 2012. She currently serves as the National Security Agency's Commandant of the National Cryptologic School, which is comprised of four colleges, to include the Colleges of Cyber and Cryptology. In her role, she manages and oversees the delivery of unique courses for the U.S. intelligence workforce, both civilian and military, in the areas of cyber, network security, cyber resilience, and encryption, ensuring a strong federal workforce to defend critical national security networks. Ms. Janosek's areas of expertise include academic leadership, privacy and technology, governance and data policy, export control, defense acquisition, information and cyber security. In

her current role, she is committed to the educational, leadership, professional and practical learning needs of the nation's cyber workforce in today's dynamic threat environment.

Mini Track Chairs

Dr. Jim Q. Chen, Ph.D. is Professor of Cyber Studies in the College of Information and Cyberspace (CIC) at the U.S. National Defense University (NDU). His expertise is in cyber warfare, cyber deterrence, cyber strategy, cybersecurity technology, artificial intelligence, and machine learning. Based on his research, he has authored and published numerous peer-reviewed papers, articles, and book chapters on these topics. Dr. Chen has also been teaching graduate courses on these topics. He is a recognized expert in cyber studies and artificial intelligence.

Dr Noluxolo Gcaza is passionate about making cybersecurity accessible to different contexts. Her research interests include cyber security governance, cybersecurity awareness and education. Currently she is a Research Group Leader at the Council for Scientific and Industrial Research (CSIR). She serves on the Advisory Board of the Center for Research in Information and CyberSecurity (CRICS) at Nelson Mandela University. Dr Gcaza also served as a Board Member in SaveTnet, a non-profit organization that focuses on fostering a culture of cyber security in a community setting through spreading cyber security awareness. She contributes in the SABS standardisation process as a committee member of the Information Security Technical Committee.

Dr Maanak Gupta is an assistant professor in computer science at Tennessee Tech University. He received his PhD from the University of Texas at San Antonio. His primary area of research includes security and privacy in cyber space. He works in machine learning and AI assisted cyber security solutions. He received the UTSA CS Outstanding Doctoral Dissertation Award in 2019. His website is: www.maanakgupta.com

Dr. Greg Laidlaw, DMIT, CISSP, C|EH, serves as the Department Chair and Lecturer in the Cybersecurity & Information Systems Department at the University of Detroit Mercy. Greg's research focuses on secure systems, secure analytics, and machine learning. Prior to transitioning into full-time academia in 2011, Greg developed an extensive range of technical and managerial experience from 25 years of IT consulting in small enterprise and local government organizations. His doctoral dissertation involved adapting agile methodologies to design and expediting a data integration project for a local Sheriff's Department.

Dr Akond Rahman is an assistant professor at Tennessee Tech University. His research interests include DevOps and Software Security. He graduated with a PhD from North Carolina State University. He won the Microsoft Open Source Challenge Award in 2016, the ACM SIGSOFT Doctoral Symposium Award at ICSE in 2018, the ACM SIGSOFT Distinguished Paper Award at ICSE in 2019, and the NC State CSC Distinguished Dissertation Award in 2020. He actively collaborates with industry practitioners from IBM, RedHat, and others. To know more about his work visit: https://akondrahman.github.io/

Dr. Char Sample is the Chief Scientist for the CyberCore division of the Idaho National Laboratory. Her research focus areas include Artificial Intelligence, Threat Intelligence, Fake News/Deception, Data Resilience, cyber-physical systems and cultural influences on cyber events and behaviors. Dr. Sample's background includes time spent in the private sector, public sector and academia. She continues to try to merge the best features from each pf these areas to guide her research.

Dr. Unal Tatar is currently an Assistant Professor of Cybersecurity at the College of Emergency Preparedness, Homeland Security, and Cybersecurity, University at Albany. He has 15+ years of cybersecurity experience of cybersecurity in government, industry and academia. He is the former coordinator of the National Computer Emergency Response Team of Turkey. Dr. Tatar's research is funded by NSF, NSA, DOD, and Society of Actuaries. Dr. Tatar holds a BSc degree in Computer Engineering, an MS degree in Cryptography and a Ph.D. in Engineering Management and Systems Engineering. His main topics of interest are cybersecurity risk management, cyber resiliency, cyber insurance, and blockchain.

Pardis Moslemzadeh Tehrani is a senior lecturer at the Faculty of Law, University of Malaya. Her research interests lie in the areas of cyberterrorism, cyberlaw, and international humanitarian law. Pardis's research has been widely published in peer-reviewed journals and she has presented papers at national and international level conferences. She is a member of the editorial review board in several journals. She is also an international scientific member of the Australian and New Zealand Society of International Law. Pardis's most recent book is Cyberterrorism: The Legal and Enforcement Issues (World Science and Imperial College Press of London, 2017).

Dr. Benjamin Yankson is an Assistant Professor of Cybersecurity at the College of Emergency Preparedness Homeland Security and Cybersecurity. He has over 15yrs experience in various technical leadership roles in Information Technology security within Healthcare and Education. He is the former Application Manager, Critical Care Information System for the province of Ontario's (CritiCall Ontario), Canada. Dr. Yankson holds a CompTIA Security+, a B.A degree in Information Technology, a master's degree in Information Technology Security (MITS), and a Ph.D. Computer Science. His current teaching and research work focuses on IoT Security, Cybersecurity Risk Management, Threat Risk Assessment (TRA), Security Auditing/Compliance, Digital Forensics, and Privacy.

Workshop Facilitator

Dr Edwin "Leigh" Armistead is the President of Peregrine Technical Solutions, a certified 8(a) small business that specializes in Cyber Security. A retired United States Naval Officer, he has significant Information Operations academic credentials having written his PhD on the conduct of Cyber Warfare by the federal government and has published three books, in an unclassified format in 2004, 2007 and 2010, all focusing on full Information Warfare. He is also the Chief Editor of the Journal of Information Warfare (JIW) https://www.jinfowar.com/; the Program Director of the International Conference of Cyber Warfare and Security and the Vice-Chair Working Group 9.10, ICT Uses in Peace and War. Shown below are the books on full spectrum cyber warfare and the JIW:

Game! Crime? The Shadow Economy Around Digital Games as a Playground for Cybercrime

Alexander Pfeiffer[1, 2, 3], Thomas-Gabriel Rüdiger[7], Stephen Bezzina[6], Simone Kriglstein[4, 5] and Thomas Wernbacher[2]
[1]Comparative Media Studies/Writing, Massachusetts Institute of Technology (MIT), Cambridge, USA
[2]Center for Applied Game Studies, Danube-University Krems (DUK), Austria
[3]Department of Artificial Intelligence, University of Malta (UoM), Msida, Malta
[4]Austrian Institute of Technology GmbH (AIT), Vienna, Austria
[5]Faculty of Computer Science, University of Vienna, Austria
[6]Ministry for Education and Employment, Floriana, Malta
[7]Cybercriminologist
alex_pf@mit.edu
mail@stephenbezzina.com
simone.kriglstein@ait.ac.at
Thomas.wernbacher@donau-uni.ac.at
thomas.ruediger@hpolbb.de
DOI: 10.34190/IWS.21.014

Abstract: The games segment is growing steadily and is a major part of the entertainment industry. In particular, the Free2Play games, or games that primarily rely on mechanics like in-game purchases which are playable on mobile devices, play an important role. In the context of virtual items, online role-playing games and multiplayer online battle arenas, still account for a significant share of total sales. The loop is completed with esports, that is competitive digital gaming for real cash prizes. As such, esports can certainly be seen as one of the major trends, and consequently a part of the gaming industry that should be in focus, with regard to potential criminal behaviour. This article discusses cybercrime in relation to digital games and its various forms. The focus of the paper is the players' perspective on the issue of cyber-crime around the world of digital games. For this purpose, a focus group with players has been conducted to discuss various aspects that have been identified through desk-research.

Keywords: cybercrime, gamecrime, cybergrooming, identity theft

1. Introduction

The latest figures from SuperData show that by 2019[1], the games industry has grown to $120.1 billion in global revenue. Despite, or perhaps because of, Covid-19, a further increase of 4% is predicted for 2020. The largest share of revenue comes from mobile games, in particular the so-called Free2Play titles, which give players access to a significant portion of their content without payment. In turn, virtual items and virtual tokens, which represent currency in games, are becoming increasingly important and at the same time more and more accepted. This has potentially led to an upsurge in the attractiveness for fraud, along with the steady annual turnover. This stems from illegal sales of virtual items, counterfeiting and the pretended sale of these assets and the hacking through malicious computer code or social engineering.

Another domain for potential cyberattacks aside from exposing, altering, disabling or gaining unauthorized access to and unlawful selling one or more assets, lies in the field of esports. A study by Green Man Gaming[2] shows that esports, that is competitive digital gaming for real cash prizes, has now reached the $1 billion annual turnover mark, with a forecast of tripling in the next five years. Many of these tournaments now take place online (also due to Covid-19). In addition to classic doping, digital doping or e-doping, is playing an increasingly important role in esports and represents a threat, in the form of cybercrime or fraud.

Other topics related to cybercrime and games include the theft of identities and credit card data, but also the misuse of in-game chat systems, for example for planning criminal activities. Last but not least, a major issue is

[1] https://www.superdataresearch.com/2019-year-in-review
[2] https://www.greenmangaming.com/de/the-money-game/

the befriending of children online and consequently the building of emotional connections with intentions of sexual abuse, exploitation or trafficking. This is known as cyber grooming. Further aspects of research in regards to crime and games, which are, however, not explicitly the aim of this specific contribution, is the area of transfer between games and real life (for instance the so-called killer game debate).

The aim of this article is thus to provide a clear overview of the problems caused by cybercrime in the gaming sector, how this is currently being manifested and ways in which it can be mitigated/solved. As such, this critical analysis is a valuable contribution to literature, as most of the research so far has been focussing exclusively on specific themes within the field and no overall view of the topic exists. Thus, the authors believe that this article is especially relevant to cybercrime experts who are not yet familiar with the games sector.

2. Research questions and methods

The goal of this article is to look at the topic of game crime from the perspective of the players, with a focus on the aspect of digital items and how they relate to the various aspects of game crime mentioned above. This leads to the following research questions.

- Which aspects of cybercrime around digital games are identified by the players?
- Which measures do players suggest in order to better protect the community?

To achieve their research goal, the authors carried out extensive desk research and conducted a focus group with five participants. The participants of the focus group are experienced players in the genres of online role playing games, multiplayer online battle arenas and mobile-phone multiplayer games and part of the broader game-studies community. The approach is to understand as explorative with the goal to identify aspects for future research.

The realization of the focus group in Table 1 is based on the method of the problem-centered interview following Witzel (1985), whilst the evaluation of the key statements was conducted according to Mayring's (2010) approach regarding content-analyses. This problem-centered approach is characterised by the orientation towards a socially relevant problem (in this case the crime in, through and around digital games) and the organisation of the cognition or learning process (pre-interpretation). As such, the interviewer uses the previous knowledge of objective (in this case the knowledge gained through desk research) in order to understand the interviewees' explications and ask questions or demands oriented towards the problem. Parallel to the production of broad and differentiated data material, the interviewer works on the interpretation of the subjective view of the interviewees opinions and refines this in view of the research problem. In the content analysis, in addition to the formation of categories, in this case the places where criminal acts occur and the way in which criminal acts manifest themselves, the authors have reduced the results of the interviews in the form of core statements.

Table 1: Participants of the focus group

Expert ID	Gender	Age
E1	male	22
E2	male	26
E3	male	45
E4	female	27
E5	female	19

3. Related research

Table 2 shows in tabular form, the relevant research projects that are related to the authors' approach. The findings formed the basis for the guided discussion and questions from the moderators in the focus group. Two of the publications listed are anthologies that look at the topic of cybercriminology from different viewpoints, often concluding that more in-depth research is required to look more closely at the role of digital games in the research discipline of cybercrime. In desk research, the changes in the possibilities for cybercrime in relation to technical and social conditions and the current trends in the game genres were particularly noticeable from 2005 to 2010 to 2015 to 2019/2020. Of particular interest here is the expansion of broadband Internet, the growth of mobile Internet, larger possible download volumes, the evolution of cell phones into high-class mobile computers and the steady growth in the number of players. This is particularly interesting in the area of participatory games and e-sports. In other words, these paved the way from the single-player world towards the multiplayer experience.

Table 2: Related research

Authors	Topic
Chen et. al. (2005)	According to their analysis of online gaming characteristics in Taiwan in the year 2005, the majority of online gaming crime is centered around theft and fraud. In fact, the crime scene was mainly rampant in internet cafés. The offenders and victims were mainly male and offenders always proceed alone. The age of offenders was quite low and 8.3 percent of offenders were under 15 years old. The offenders were mostly students and unemployed, with most of them (81.9 percent) not having criminal records. The type of game giving rise to most of the criminal cases was Lineage Online (93.3 percent). The average value of the online gaming loss was about US$ 459.
Krebs and Rüdiger (2010)	The book Gamecrime and Metacrime deals with questions like: Is there criminality in connection with virtual worlds? What are the manifestations. What is the difference between bright (reported to the authorities) and dark (not reported) field? It can be seen as one of the first explorative works on this topic in the German-speaking world and a pioneering fundamental work with a focus on criminal law.
Rüdiger and Pfeiffer (2015)	The anthology "Game!Crime?" offers a wide spectrum of articles in regards to the topic of crime in and around video games. The contributing authors deal with topics such as griefing in digital games, how does mass media report about games?, the future of the leisure industry, online addiction, metaworlds and cybercrime, free2play games and cyber-grooming among others.
Brewis (2019)	Brewis conducted a focus group to identify aspects of crime from and around video games. She concludes: *"This work has found that constructions of crime in video games are complex, predominantly focused on the aim of the particular game, from satire to empathy and education. Further, it was found among the games examined that there is a recipe within video games for creating an ideal scenario to allow generally law-abiding individuals to commit fictional virtual crime. Identifying conditions that allow individuals to behave in a criminal or deviant way may have real world applications in understanding criminal behavior which further research may be able explore."*
Craig et. al. (2020)	The anthology "Video Games, Crime and Next-Gen Deviance" aims to reorienting the debate on video game related crimes. The contributing authors deal with topics such as online addiction, sexual violence, violence in and around games or the phenomenon of swatting.

4. Results

The following section describes the key points with regard to crime in, around and within games that have been identified in the focus group discussion. The presentation is carried out according to the identified areas where and how cybercrime occurs in, around and within digital games. In each section the core problem was then identified and summarized, and a possible solution was outlined. As already mentioned, this comprehensive overview is particularly useful for experts in the field of cybercriminology, who do not consider themselves as games experts or familiar enough with the world of gaming.

Identity Theft

Identified problem: The first acknowledged problem is identity theft, either with the help of technical aids, social engineering or the creation of fake login pages. This information is quite often used to start fraudulent activities inside or outside the game, such as to get into another system (such as a bank account) or to sell data on the dark web.

Possible solutions: Game manufacturers, distributors, online sale-portals, the classic media, but also the public authorities have to organise more educational campaigns in order for the players to know more about this problem, learn which red flags to watch out for when inputting data on the internet or when a stranger's avatar starts asking personal questions about real life.

Credit card theft

Identified problem: Similar to the first aspect, credit card theft is about achieving immediate financial gain. Often the good-naturedness of the players is exploited here, or rather their greed to quickly achieve success. For example, websites offer level-up services, where not only the account data but also the credit card data is entered in a supposedly secure way. This can happen for instance when digital items like skins in League of Legends or digital currencies like gold in World of Warcraft are sold on illegally operated trading platforms.

Possible solutions: The solution is similar to the previous aspect. As for the issue of identity theft, massive education amongst the gaming community is necessary, coupled with harder bans for players who buy or sell illegal digital assets. Gaming companies must also pursue these cases more vigorously and not perhaps even be pleased if the scammers, for example, start a character transfer to another server for real money.

Theft of virtual goods

Identified problem: Stealing virtual goods can be a way to sell them as illustrated in the previous example. In the previous example, the sales listing is used to steal credit card data, but of course there is also trading on regular virtual asset platforms. This applies to games where trading is allowed, and the infrastructure is available. Nevertheless, the virtual goods traded there can of course be acquired irregularly, for example by exploiting hacked accounts. Again, this is related to the first identified aspect, where identity theft is committed in the hope of getting access to account data in order to rob the victim's character and sell the virtual goods. Virtual goods and their trading could also be an issue with respect to money loundering. Another related aspect is acquisition crime, where the money made through the selling of virtual items is needed to cover, for example, the costs for drug addiction.

Possible solutions: A proposed solution is that game operators do not immediately replace stolen goods. Instead, digital forensics should be used to try to reverse the perpetrator's transactions. And there must be an understanding that virtual theft is also a crime. The rate between cases reported to the police and actual crimes must decrease. New technical possibilities such as Blockchain should also be taken into account if applied properly.

Meetings concerning illicit activities

Identified problem: The in-game chat can be used to discuss illegal activities outside the chats on the police radar. This can begin by planning a crime. But also activities of the Nazis from the second world war could be approved through the game chat, a criminal act in countries like Austria or Germany. While major games are aware of this problem, there are of course countless independent games that do not have the possibility to interpret the chats of the users.

Possible solutions: Game masters have to show that they are paying attention to the chat and that illegal activities are detected. This is where Artificial Intelligence and text analysis can also be helpful.

Mobbing and insulting offences

Identified problem: The chat can also be used to insult other players. This has to be prevented and stopped, especially if such insults are addressed towards aspects outside of the game world.

Possible solutions: As with the previous aspect, the moderators and game masters must intervene more strongly. Mechanisms from behavioural science, like nudging, can also be possibly used.

5. Conclusion and identified aspects for future research

This paper aims to contribute knowledge and research towards the initiation of discussion surrounding the fields of cybercrime and gaming. The game experts from the focus group have identified a number of different factors, which also correspond to themes in the reviewed literature. In conclusion and as a general overview for future research, the authors propose three concrete recommendations with regard to this domain:

- Definition of the area of crime surrounding digital games as a separate research discipline in which criminologists conduct interdisciplinary research with specialists from the field of game studies;
- Cooperation between game companies and authorities, especially youth protection institutions, based on scientific data and analysis;
- Access to research findings by the relevant stakeholders and consequently the design, development and implementation of concrete solutions.

References

Brewis, E. (2019) Crime Doesn't Play: A Study of the Construction of Crime in Popular Video Games, 10.13140/RG.2.2.23058.89281

Chen, Y., Chen, P.S., Hwang, J., Korba, L., Song, R. and Yee, G. (2005), An analysis of online gaming crime characteristics, Internet Research, Vol. 15 No. 3, pp. 246-261. https://doi.org/10.1108/10662240510602672

Craig, K., Lynes, A., Hoffin, K. (eds) (2020) Video Games, Crime and Next-Gen Deviance, emerald Publishing UK, Bingley

Krebs, C., Rüdiger, T.-G. (2010) Gamecrime und Metacrime, Strafrechtliche relevante Handlungen im Zusammenhang mit virtuellen Welten. Verlag für Polizeiwissenschaft, Frankfurt

Mayring, P. (2010) Qualitative Inhaltsanalyse; Grundlagen und Techniken, Beltz Verlag, Weinheim, Basel

Rüdiger, T.-G., Pfeiffer, A. (eds) (2015) Game!Crime? Verlag für Polizeiwissenschaft, Frankfurt

Witzel, A. (1985) Das problemzentrierte Interview. In Qualitative Forschung in der Psychologie : Grundfragen, Verfahrensweisen, Anwendungsfelder, Gerd Jüttemann (Ed.). Beltz, Weinheim, 227–255

View publication stats