5. Annual Human Factor in Cybercrime Conference

von Joline Wochnik und
Dr. Nicole Selzer[*]

I. Einleitung

Die 5. Annual Human Factor in Cybercrime Conference (HFC) fand vom 10. bis zum 12. September 2023 im Festsaal des neugotischen Stadthauses der Stadt Halle (Saale) statt. Sie wurde von der Agentur für Innovation in der Cybersicherheit GmbH (nachfolgend: Cyberagentur) in Kooperation mit lokalen Partnern aus den Niederlanden, The Hague University of Applied Sciences, Vrije Universiteit Amerstam und dem NSCR, ausgerichtet. Zum internationalen Organizing Committee der HFC zählen *Tamar Berenblum* (Israel), *Cassandra Cross* (Australien), *Benoît Dupont* (Kanada), *Thomas Holt* (USA), *Rutger Leukfeldt* (Niederlande), *Nicole Selzer* (Deutschland) und *Marleen Weulen Kranenbarg* (Niederlande)[1].

Die HFC wurde von *Tamar Berenblum* (ZI) und *Rutger Leukfeldt* (The Hague University of Applied Sciences/NSCR) ins Leben gerufen und fand erstmals 2018 in Jerusalem statt.[2] In den darauffolgenden Jahren wurde sie in Amsterdam (2019)[3], virtuell in Montreal (2020), in Clear Water, Florida (2022) und in Halle/Saale (2023) abgehalten und ist für 2024 wiederum in Montreal vorgesehen.

Die zweieinhalb-tägige internationale Konferenz, mit jährlich wechselnden Standorten, hat sich empirische Spitzenforschung, fachlichen Austausch und Kooperation zum Ziel gesetzt. Im Fokus der Konferenz steht die wissenschaftliche Auseinandersetzung mit dem menschlichen Faktor der Cyberkriminalität. Die Konferenz adressiert Wissenschaftlerinnen und Wissenschaftler sowie Praktikerinnen und Praktiker verschiedenster Disziplinen der Bezugswissenschaften der Kriminologie, wie Soziologie, Psychologie, Anthropologie, Rechts- und Wirtschaftswissenschaften, aber bspw. auch Informatik und weitere mehr. Um den Gedanken der Spitzenforschung voranzutreiben, sind Teilnehmerinnen und Teilnehmer gehalten, aktuelle Forschungsergebnisse mit einer stark empirischen Komponente und einem provokativen bzw. herausfordernden Ansatz zu präsentieren, die innovative empirische Perspektiven für die cyberkriminologische Forschung bieten.

Bei der 5. HFC in Halle (Saale) wurden in mehreren Sessions á drei bis vier Vorträge die verschiedenen Arten und Ursachen von Cyberkriminalität sowie Viktimisierung und entsprechende Auswirkungen, das institutionelle Umfeld, Vorschriften und deren Durchsetzung thematisiert. Auch ein Roundtable mit Vertreterinnen und Vertretern von Sicherheitsbehörden und der Polizeiforschung gehörte zum Programm, darunter *Prof. Dr. Johannes Fähndrich* (Hochschule für Polizei Baden-Württemberg), *Lukas Hardi* (ZITiS), *Louis Jarvers* (Programm Polizei 20/20), *Volker Peters* (LKA Niedersachsen) und *Dr. Patrick Voss - de Haan* (BKA). Sie erörterten die Sichtweise, Herausforderungen und Bedarfe aus Strafverfolgersicht. Diskutiert wurde u.a. darüber, welcher Schaden durch Cyberkriminalität wirklich angerichtet werde sowie welche forensischen Methoden notwendig sind, um Cyberkriminalität aufzuklären und wie Ressourcen bestmöglich eingesetzt werden sollten. Zudem wurde betont, wie wichtig es sei, zukünftige Trends und Entwicklungen im Bereich der Cyberkriminalität zu identifizieren und Mechanismen zu entwickeln, um die Effizienz von Maßnahmen zu messen und die digitale Kompetenz gesellschafts- und institutionsübergreifend auf- und auszubauen. Der Roundtable stellte gleichsam die Handshake-Veranstaltung zur Eröffnung des Network-Events „{ Cyber : Crime || Security || Society }“ dar, welches im Anschluss an die HFC ebenfalls in Halle (Saale) stattfand und von der Cyberagentur erstmalig ausgerichtet wurde.[4]

Um dem Auftrag der Cyberagentur, innovationsorientierte Forschung im Bereich der Cybersicherheit und diesbezüglicher Schlüsseltechnologien in der Inneren und Äußeren Sicherheit anzustoßen und in besonderer Weise auch dem Themenschwerpunkt Cyberresiliente Gesellschaft Rechnung zu tragen, wurde bei der 5. HFC das Thema Zukunftsforschung beleuchtet. Ziel des von der Cyberagentur durchgeführten „Futurology“-Workshops war es, den kriminologischen Blickwinkel neu auszurichten und zu antizipieren, welche Themen zukunftsträchtig sind und wo angesetzt werden kann, um Cyberkriminalität von übermorgen zu begegnen, Strafverfolgungsbehörden zu stärken und die Resilienz der Gesellschaft zu fördern.

Für die 5. HFC gingen 57 Bewerbungen aus zwölf Ländern ein, darunter Australien, Dänemark, Deutschland, Großbritannien, Italien, Kanada, die Niederlande, Portugal, der Schweiz, Spanien, Tschechien und den USA. Schlussendlich stellten 33 Vortragende[5] aus neun Ländern in General und PhDs Sessions ihre Forschungsarbeiten

* Die Verfasserinnen sind Forschungsreferentinnen in der Abteilung Sichere Gesellschaft in der Agentur für Innovation in der Cybersicherheit GmbH in Halle (Saale).

1 Die letzten drei Personen stellten 2023 das local organizing committee.

2 *Selzer*, Kriminalistik 2019, 223 ff.

3 *Moneva*, in: *Weulen Kranenbarg/Leukfeldt*, Cybercrime in Contect: The human factor in victimization, offending, and policing, Bd. 1, 2021, 5 ff.

4 *Wochnik/Selzer*, Kriminalistik 2024, 215-218.

5 Anmerkung: Nicht alle Referenten haben die Freigabe für den Konferenzreport erteilt. Zudem werden hier nur die Vortragenden genannt und nicht alle Autoren der eingereichten Beiträge.

vor, die sich auf unterschiedliche Themenfelder der Cyberkriminalität und Cybersicherheit konzentrierten. Auch Vertreterinnen und Vertreter vom BKA, vom UK Homeland Security und dem Interventionsteam COPS der niederländischen Polizei nahmen an der Veranstaltung teil.

II. Täter & Phänomenbereiche

Bei der Betrachtung der Täter und Phänomenbereiche im Kontext der Cyberkriminalität konzentrierten sich die Forschenden vor allem darauf, wer die Täter bzw. Tätergruppen sind und was diese charakterisiert.

Es wurden Forschungsergebnisse zu den Wegen junger Menschen in und aus der Cyberkriminalität vorgestellt sowie die Entwicklung des Interesses und der Motivation untersucht. Dabei bildete sich in einer von *Joeri Loggen* (NSCR / Universiteit Utrecht) vorgestellten Forschungsarbeit der Trend ab, dass Jugendliche zunehmend in Cyberkriminalität verwickelt sind und Straftaten dabei zumeist in Gruppen begehen. Vor allem das schnelle Geldverdienen stehe dieser Untersuchung zufolge im Fokus der Jugendlichen.

Rubén Fernandez (Valencia Local Police) stellte unter anderem das Projekt CC-DRIVER vor, welches die menschlichen und technischen Antreiber der Cyberkriminalität mit besonderem Schwerpunkt auf Jugendkriminalität und Cybercrime-as-a-Service untersucht. Ziel war die Analyse neuer Formen der Kriminalität sowie die Entwicklung innovativer Instrumente zur Verhinderung, Untersuchung und Eindämmung von Cyberkriminalität.

Die von *Rutger Leukfeldt* (The Hague University of Applied Sciences / NSCR) vorgestellte Studie basiert auf 34 Interviews mit sog. Hacktivisten aus 23 verschiedenen Netzwerken. Die Studie zeigt, dass Hacktivisten auf unterschiedlichen Ebenen der Raffinesse agieren. Sie agieren aus kleinen Teams mit wenigen Mitgliedern bis hin zu größeren Kollektiven, die Dutzende von Mitstreitern zählen. Obwohl es Unterschiede zwischen den Netzwerken gibt, ließ sich im Allgemeinen eine Arbeitsteilung feststellen. Interne Regeln sowie spezifische Prozesse zur Auswahl der Ziele und zur Vermittlung der Botschaften seien erkennbar. Die Mitglieder der Netzwerke scheinen von bestimmten Freiheitsgraden zu profitieren, die eher auf horizontale als strikt hierarchische Strukturen hindeuten. Die Flexibilität in den organisatorischen Aspekten scheint in Hacktivismus Netzwerken ein Schlüsselelement zu sein.

Die von *Thomas Holt* (Michigan State University) vorgestellte Studie zu Cyberkriminellen-Netzwerken basiert auf zehn detaillierten Analysen von abgeschlossenen Verfahren u. a. im Vereinigten Königreich. Die Studie betrachtet zwei nigerianische Netzwerke, welche sich auf unterschiedliche Cyberstraftaten fokussieren. Anhand dieser beiden Fallstudien wurde untersucht, ob die zugrunde liegenden Netzwerkstrukturen und -abläufe bei diesen beiden Geschäftsmodellen ähnlich sind oder nicht. Die Analyse ermöglicht einen Einblick in die organisatorischen Strukturen und Zusammenhänge innerhalb dieser Netzwerke, was wichtige Impulse für präventive Maßnahmen und Sicherheitsstrategien liefert.

C. Jordan Howell (University of South Florida) präsentierte eine Bewertung der Bedrohungen durch Hacker im Darknet. Hacking-Dienste und -Produkte scheinen ihm zufolge zwar preislich zu variieren, seien aber in der Regel zugänglich und erschwinglich und bieten häufig sogar individuelle Anpassungsmöglichkeiten. Die Studie warf Licht auf die Bedrohung der durch das Darknet ermöglichten Hackings für US-Vermögenswerte und schloss mit einer Diskussion über innovative automatisierte Methoden zur Vorhersage und Verhinderung von Cyberangriffen, die durch Darknet-Marktplätze ermöglicht werden.

Auch *Patricia Saldaña-Taboada* (Universidad de Granada) beschäftigte sich mit Darknet-Marktplätzen. Sie untersuchte die Attraktivität von Bitcoins für kriminelle Aktivitäten und führte eine qualitative Analyse eines Darknet-Forums über Kryptowährungen durch. Die Ergebnisse unterstreichen, dass nicht die Wahl der Kryptowährung für Cyberkriminelle entscheidend ist, sondern die Schaffung von Umwegen, um die Rückverfolgbarkeit zu vermeiden.

Bianca Steffes und *Anna Zichler* (Universität Saarland) diskutierten virtuelle Vergewaltigungen und Sexualdelikte im Metaverse. Sie beschäftigten sich mit der Klärung der Frage, ob derartige Delikte als Cyberkriminalität bezeichnet werden können bzw. ob eine Sexualstraftat ohne Körperkontakt begangen werden und inwieweit ein Avatar Opfer einer Sexualstraftat sein kann. Die Präsentation beleuchtete rechtliche und psychologische Überlegungen sowie technische Maßnahmen zum Schutz von Nutzern vor sexuellen Übergriffen in virtuellen Welten.

Julia Katherina Mahnken (Universität Hamburg) befasste sich damit, wie sich ein klassisches Kriminalitätsphänomen unter digitalen Bedingungen verändert. Dafür erweiterte sie die Analyse einer Online-Drogenplattform um den Kontext langfristiger sozialer Prozesse, um einen methodologischen Punkt zu machen. In ihrer Analyse geht sie der Frage nach, inwieweit unter einer sozio-historischen, prozessorientierten Linse Wechselwirkungen zwischen verschiedenen Dimensionen (digitaler) Kriminalität sichtbar werden. Mit Blick auf unterschiedliche Ebenen, wie Konsumenten, Tatbeteiligte, Ermittlungsbehörden und Gesellschaft, ließen sich in der erweiterten Perspektive sowohl resultierende Innovationswiderstände als auch mögliche spezifische Veränderungschancen ableiten. Es zeigte sich, dass erstaunlich wenig „neu“ ist. Vielmehr wurde in der Analyse sichtbar, wie sich bestehende Bedürfnisse und Strukturen unter digitalen Bedingungen fortsetzen. Da die Analyse freilegt, wie eine angenommene Neuheit die Sicht versperren kann, argumentierte sie daher methodologisch, dass die (digitalen) Transformationen des Sozialen, der Objekte und der Beziehungen als konstitutive Bestandteile der Kriminalität betrachtet werden sollten. Dafür schlug sie vor, künftig den Analysefokus auch auf die Transformationen von Kriminalität zu legen und ihre sich ebenfalls unter digitalen Bedingungen

verändernden Kontexte in die Analyse stärker einzubeziehen.

III. Opfer & Viktimisierung

Neben der Betrachtung der Täter lag ein weiterer Fokus der Forschenden auf den Opfern der Cyberkriminalität und den Aspekten der Viktimisierung.

Danielle Stibbe (NSCR/ Universiteit Utrecht) stellte ihre Forschungsarbeit bezüglich der Opferauswahl im Kontext des unbefugten Zugriffs auf Konten vor und besprach dabei den Prozess der Auswahl von Opfern und dessen Beeinflussung durch die Abwägung von Kosten und Nutzen (Rational Choice Approach).

Susanne Van 't Hoff-de Goede (The Hague University of Applied Sciences) fokussierte sich auf Interviews mit Opfern von Online-Betrug, um Einblicke in deren Erfahrungen vor, während und nach dem zivilrechtlichen Verfahren zu gewinnen, das neuerdings in den Niederlanden auch ohne ein vorangegangenes oder paralleles Strafverfahren praktiziert wird. Die Untersuchung zeigt, dass die Gründe für die Einleitung solcher Verfahren naturgemäß variieren und von dem einfachen Wunsch nach Rückerstattung, über die Konfrontation des Täters bis hin zur Verhinderung zukünftiger Vorfälle reichen. Die Besonderheit der Untersuchung ist jedoch, dass die Opfer in den meisten Fällen die Entschädigungszahlung nicht vom eigentlichen Täter, sondern vom sog. „Geldesel" (money mule), über dessen Konto der Betrug und das Geld des Opfers als Zwischenstation lief, erhielten bzw. diejenige Person zur Verantwortung gezogen wurde, da die eigentlichen Täter oftmals nicht identifiziert werden können.

Michael Levi (Cardiff University) beschrieb in seinem Vortrag die öffentlichen und privaten Maßnahmen, die ergriffen werden, um Betrügereien zu bekämpfen und die Angst vor Betrug zu verringern. Die Ergebnisse seiner Forschungsstudien unterstreichen die Notwendigkeit von evidenzbasierten Reaktionen auf Veränderungen bei cybergestützten Betrugsmustern, einschließlich Strafverfolgungs- und Gesundheitsmaßnahmen sowie Werbung zur Betrugsbekämpfung für die Öffentlichkeit und Unternehmen.

Inês Sousa Guedes (Universidade do Porto) betrachtete die Angst vor Cyberkriminalität und untersuchte, ob diese Angst je nach der spezifischen Form der Bedrohung, ob sachbezogene oder interpersonelle Cyberkriminalität, variiert. Die Untersuchung zeigt, dass der größte Prädiktor für beide Bereich die Angst vor Kriminalität im Allgemeinen ist und die Angst vor sachbezogener Cyberkriminalität die der interpersonellen übersteigt.

Stefan Sütterlin (Hochschule Albstadt-Sigmaringen) beschäftigte sich in seiner vorgestellten Untersuchung mit dem Zusammenhang zwischen Viktimisierung und dem mentalen Zustand der Betroffenen von Cyberkriminalität. Hierbei zeigte er, dass die Überschätzung der eigenen Fähigkeiten sowie die Unterschätzung der eigenen Anfälligkeit für Manipulation durch böswillige Akteure wesentlich zur Viktimisierung durch Cyberkriminalität beiträgt.

Pia Hüsch (Royal United Services Institute) richtete den Fokus auf die direkt oder indirekt betroffenen Opfer von Ransomware-Angriffen. Die Präsentation hob die menschlichen Auswirkungen hervor und bot neue Einblicke in die Erfahrungen der Opfer sowie den weitreichenden Schaden, den Einzelpersonen durch Ransomware-Angriffe erleiden. Die Ergebnisse der vorgestellten Studie zeigen ein breites Spektrum von Auswirkungen, einschließlich solcher auf die psychische Gesundheit und physische Beeinträchtigungen, die die Opfer sowohl kurz- als auch langfristig erleben. Basierend auf diesen Erkenntnissen wurden evidenzbasierte politische Empfehlungen ausgesprochen, die darauf abzielen, den Schaden für Ransomware-Opfer zu minimieren.

Ebenfalls zum Themenbereich Ransomware präsentierte *Sifra Matthijsse* (The Hague University of Applied Sciences) eine Studie, die darauf abzielt, das Verhalten kleiner und mittelständiger Unternehmen (KMU) nach einer Ransomware-Viktimisierung zu verstehen. Die Ergebnisse dieser Studie zeigen, dass die Wahrscheinlichkeit, dass KMUs das Lösegeld zahlen, im Allgemeinen gering ist. Entscheidende Faktoren für eine Zahlung scheinen nicht die (geringe) Höhe des geforderten Lösegeldes zu sein, sondern die Empfehlung eines Cybersicherheitsunternehmens, das Lösegeld zu zahlen sowie das Fehlen eines Backups.

Auch *Noelle Warkentin* (Simon Fraser University) beschäftigte sich in ihrer Präsentation mit den ernsthaften und wachsenden Auswirkungen von Ransomware auf Unternehmen. Sie stellte fest, dass neben den finanziellen Verlusten Ransomware auch die Produktivität des Unternehmens und der Mitarbeiter erheblich beeinträchtigt.

IV. Cybersicherheit und Polizeiarbeit

Auch die andere Seite der Cyberkriminalität wurde auf der Konferenz in den Fokus gerückt. Verschiedene Experten lieferten Vorträge zum Thema der Cybersicherheit und Cyberhygiene.

Sascha Fahl (CISPA Helmholtz-Zentrum für Informationssicherheit) beleuchtete in seinem Vortrag die Herausforderungen, denen KMUs in Bezug auf Cybersicherheit gegenüberstehen. Dazu betrachtete er den Einsatz von technischen und organisatorischen Sicherheitsmaßnahmen in KMUs. Die Forschung zeigt, dass viele Unternehmen bereits technische Sicherheitsmaßnahmen implementiert haben, jedoch Unterschiede in der Meldung von Cyberkriminalitätsvorfällen aufgrund von Industriesektor, Unternehmensgröße und Sicherheitsbewusstsein bestehen. Fahl schloss die Präsentation mit Empfehlungen für zukünftige Forschung, Industrie und politische Entscheidungsträger.

George Burruss (University of South Florida) fokussierte sich in seinem Vortrag auf Cyberhygiene-Praktiken. Er

untersuchte die Bereitschaft zur Änderung von Verhaltensweisen bei Kenntnis des generellen Risikos, Opfer von Identitätsdiebstahl zu werden. Die Untersuchung betont die Notwendigkeit maßgeschneiderter Cybersicherheitsausbildungen, die auf den individuellen Merkmalen der Nutzer basieren, anstatt auf einem Einheitsansatz.

Russell Brewer (The University of Adelaide*)* präsentierte ein automatisiertes Softwaresystem, welches biometrische Merkmale aus Material von sexuellem Kindesmissbrauch extrahiert und die extrahierten Merkmale mit Datenbanken abgleicht. Mittels Netzwerkanalyse konnten Verbindungen zwischen den in den Filmen dargestellten Tätern veranschaulicht werden, wodurch diese Arbeit nicht nur neue Einblicke in die soziale Organisation dieser Straftaten und Straftäter liefert, sondern auch praktische Auswirkungen auf die Strafverfolgung hat.

V. Futurology-Workshop

Der Futurology-Workshop, den die Cyberagentur im Zuge der HFC ausrichtete, war in zwei Sessions aufgeteilt. Das Ziel der Sessions war die Identifizierung von potenziellen zukünftigen Forschungsrichtungen sowie die Vernetzung der Teilnehmenden untereinander. In der ersten Session, die zugleich als Ice-Breaker am ersten Tag diente, sollten die Teilnehmenden in wechselnden Zweierkonstellationen über die zukünftige Entwicklung von Cyberkriminalität diskutieren. In der ersten Runde galt es zu identifizieren, welche gegenwärtigen Trends sich abzeichnen und wie sich Cyberkriminalität in den kommenden fünf bis zehn Jahren entwickeln könnte. In der zweiten Runde sollten anhand der fünf PESTL-Dimensionen Politik, Wirtschaft, Soziales & Ethik, Technologie und Recht die identifizierten Entwicklungen betrachtet und bewertet werden. In der letzten Runde galt es Wild Cards zu identifizieren, also Ereignisse, die eine geringe Wahrscheinlichkeit des Eintretens haben, aber einen umso größeren Impact. In der zweiten Futurology-Session wurden die Teilnehmenden in fünf Gruppen aufgeteilt und jeder Gruppe eine der fünf PESTL-Dimensionen zugewiesen. Diskutiert wurde, inwieweit die einzelnen Dimensionen zukünftige Cyberkriminalität und Cybersicherheit beeinflussen und wie dies konkret geschehen könnte. Herauskristallisierten sich die folgenden Schwerpunkte: Ressourcenknappheit, geopolitische Entwicklungen, Künstliche Intelligenz als Mainstream, die Moderation von Inhalten auf sozialen Plattformen, die Gefährdung des Finanzmarktes und von Regierungseinrichtungen sowie die Notwendigkeit von Ethik und Werten im digitalen Kontext. Die Haupterkenntnisse der einzelnen Gruppendiskussionen wurden am Ende vorgestellt und mittels Graphic Recording visualisiert.

VI. Fazit

Die HFC erfreut sich zunehmender Beliebtheit und hat 2023 einen Bewerberrekord erzielt. Die Qualität der eingereichten Beiträge übersteigt die der herkömmlichen kriminologischen Veranstaltungen, wie die European und American Society of Criminology (ESC & ASC)[6], da bei Letzteren sämtliche Einreichungen auch unabhängig vom Stadium akzeptiert werden. Bei der HFC hingegen müssen sog. Full Paper vor Konferenzstart eingereicht werden und es herrscht ein Wettbewerbscharakter durch die begrenzte Teilnehmerzahl. Das Social Networking um die Konferenz herum trägt zu einem intensiven Feedback, Austausch und neuen Kooperationen bei. Die wechselnden Standorte begünstigen zudem den Aufwuchs der Community, da hierdurch auch lokal ansässige Wissenschaftlerinnen und Wissenschaftler auf die Konferenz aufmerksam werden. 2023 wurden vier Beiträge aus Deutschland akzeptiert. Zudem konnten auch verschiedene nationale und internationale Vertreterinnen und Vertreter von Strafverfolgungsbehörden der Konferenz beiwohnen, was gegenseitig großen Anklang fand.

Zur 5. HFC erscheinen voraussichtlich 2024 zwei Special Issues – im European Journal of Criminology (Herausgeber *Marleen Weulen Kranenbarg, Rutger Leukfeldt und Nicole Selzer*) und im Journal Deviant Behavior (Herausgeber *Thomas Holt*).

Die 6. Annual Human Factor in Cybercrime Conference findet vom 29. September bis 1. Oktober 2024 in Montreal, Kanada statt und wird von *Prof. Benoît Dupont* und *Prof. Masarah Paquet-Clouston* (local organizing committee) ausgerichtet.[7]

[6] *Reinholz/Selzer*, Kriminalistik 2020, 271-275.

[7] https://www.hfc-conference.com/call-for-papers.