Expertenmeinungen über Bildung zur IT-Sicherheit: Was jeder Mensch wissen sollte!

Ulrike Schott-Maire[1] Manuel Riel[2] Ralf Romeike[3]

Abstract: In der „digital vernetzten Welt" stellen wöchentliche Berichte über „data breaches", „gestohlene" Passwörter und gehackte Systeme – gerade in Zeiten von täglichen Videokonferenzen und Home-Schooling – alle Mitglieder unserer digitalen Gesellschaft vor die Frage, wie sie sich, ihre Daten und ihre digitale Identität schützen können. Allgemeinbildender Informatikunterricht versucht derartige Herausforderungen im Spannungsfeld zwischen gesellschaftlichen, fachlichen und wirtschaftlichen Ansprüchen zu adressieren: Um zur Klärung dieser impliziten Forderungen beizutragen, befragen wir in diesem Beitrag ausgewählte Expert*innen der IT-Sicherheit aus Wissenschaft und Wirtschaft nach den grundlegenden Konzepten, Begriffen und Ideen, die sie für jeden Menschen als relevant erachten, und vergleichen diese Expertensicht mit dem aktuellen Stand internationaler Bildungsstandards und Rahmenlehrpläne. Die Ergebnisse zeigen, dass die Schwerpunktsetzung der Expert*innen und der Curricula in etlichen Punkten erheblich divergieren: Es besteht hier weiterer Forschungsbedarf, das Themenfeld im Informatikunterricht neu zu denken. Die Kernaussagen der Expert*innen liefern überdies eine Grundlage zu einer weiterführenden didaktischen Strukturierung der IT-Sicherheit sowie zur Ermittlung von Kandidaten für Schlüsselprinzipien und -begriffe.

Keywords: IT-Sicherheit; Experteninterviews

1 Motivation

Gekaperte Nutzeraccounts, entwendete Zahlungsdaten und durch Viren, Trojaner oder Cryptolocker verursachte Systemausfälle sind in Form der beinahe täglichen Berichterstattung der Medienlandschaft (mindestens) indirekt im Alltag aller Menschen – und durch aktuelle „Cyberattacken" auf Schulportale sogar direkt – im Alltag von Lehrer*innen und Schüler*innen angekommen. Diese Vorfälle bezeugen sowohl auf individueller wie auch auf gesamtgesellschaftlicher Ebene die Herausforderungen, sowie die Relevanz von Fragestellungen der IT-Sicherheit in der vernetzten Welt. Herausforderungen, die allgemeinbildender Informatikunterricht im Spannungsfeld zwischen gesellschaftlichen, fachlichen und wirtschaftlichen Ansprüchen zu adressieren versucht. Für das Fachgebiet der IT-Sicherheit zeigen aktuelle, internationale Praxisberichte, dass Lehrkräfte das Thema als sehr wichtig empfinden und einen großen Bildungsbedarf für ihre Schüler*innen, aber auch für sich selbst sehen: Das Themenfeld sei nicht ausreichend in den Curricula repräsentiert und didaktisch nicht hinreichend im allgemeinbildenden Kontext erschlossen [PHR20]. Um sich daher aus

[1] FU Berlin, Didaktik der Informatik, Königin-Luise-Str. 24-26, 14195 Berlin, ulrisyy@zedat.fu-berlin.de
[2] FU Berlin, Didaktik der Informatik, Königin-Luise-Str. 24-26, 14195 Berlin, manuel.riel@fu-berlin.de
[3] FU Berlin, Didaktik der Informatik, Königin-Luise-Str. 24-26, 14195 Berlin, ralf.romeike@fu-berlin.de

doi:10.18420/infos2021_f258

einer gesellschaftlich-fachlichen Perspektive im Sinne der Didaktischen Rekonstruktion [PHR20] der Klärung der Ansprüche an Informatikunterricht hinsichtlich der IT-Sicherheit nähern zu können, werten wir in diesem Beitrag explorative Interviews mit Expert*innen aus verschiedenen Tätigkeitsfeldern rund um das Themengebiet der IT-Sicherheit aus.

2 Forschungsstand

Die Fragestellung, was über IT-Sicherheit bekannt sein sollte, ist im Bereich universitärer Bildung ein international akut diskutiertes Thema und führte bereits zur Entwicklung verschiedener Kompetenz- und Mapping-Frameworks: Die Anzahl und Organisationsarten der verschiedenen Akteur*innen – von wissenschaftlichen Gesellschaften, wie ACM und IEEE, bis hin zu Behörden, wie der NSA – impliziert hier bereits, welche unterschiedlichen Blickwinkel und Ansprüche an die (Aus-)Bildung im Bereich der IT-Sicherheit herangetragen werden. So bestätigt beispielsweise eine aktuelle Übersicht mit Vergleich verschiedener dieser Strukturierungsansätze des Themenfeldes [FB20], dass es bisher keinen Konsens über zentrale Inhalte und deren Gewichtung in tertiären Curricula gibt, sondern konstatiert eine starke Abhängigkeit von der jeweils eingenommen Perspektive auf das Themenfeld. Gemeinsam ist diesen Frameworks jedoch die Fokussierung auf die Frage, was (künftige) Spezialistinnen und Spezialisten im Bereich der IT-Sicherheit im Kontext tertiärer Bildung wissen sollten – nicht aber, was für alle Menschen relevant ist. Lediglich das CyBOK-Projekt (Cyber Security Body of Knowledge) der University of Bristol nimmt auch explizit die Sekundarstufe an allgemeinbildenden Schulen – und somit zumindest implizit die Fragestellung, was alle Menschen über IT-Sicherheit wissen sollten – mit in den Blick [Ra18]. Das CyBOK-Framework wird dabei mit offener Community-Partizipationsmöglichkeit im Austausch von Wissenschaft und Wirtschaft kontinuierlich (weiter-)entwickelt und strukturiert das Themenfeld der IT-Sicherheit in 19 kleinere Fachbereiche, so genannte „knowledge areas“, und fasst diese wiederum in fünf größeren Kategorien („broader categories“) zusammen.

Im Gegensatz zu den tertiären Curricula für spätere Spezialist*innen, die unterschiedliche Schwerpunkte hinsichtlich der IT-Sicherheit setzen [FB20], zeigt sich bei der Analyse schulischer Curricula ein einheitliches Bild: Selbst auf internationaler Ebene werden Themenfelder, wie „Human Factors“, nicht weiter betrachtet, während andere Themen, z. B. die Kryptographie, in fast allen der analysierten Lehrpläne vertreten sind [RR20]. Diese Ergebnisse werfen vor dem Hintergrund von Workshop-Berichten mit Lehrer*innen [PHR20], welche bei Schüler*innen – aber auch bei sich selbst – einen über aktuelle Curricula hinausgehenden Bildungsbedarf im Bereich der IT-Sicherheit sehen, die Frage auf, inwieweit allgemeinbildender Informatikunterricht der Vielzahl an gegenwärtigen Herausforderungen im Alltag gerecht wird.

3 Methodik

Wir untersuchen in diesem Beitrag die beiden folgenden Forschungsfragen:

1. Welche Ideen, Konzepte und Begriffe der IT-Sicherheit sollten aus Expertensicht alle Menschen kennen?
2. Wie deckt sich die inhaltliche Schwerpunktsetzung der Expert*innen mit den Schwerpunkten in aktuellen (Rahmen-)Lehrplänen?

Grundlage der Untersuchungen bilden die Einschätzungen von sieben internationalen Expert*innen aus Wissenschaft und Wirtschaft. Bei der Auswahl der Fachpersonen wurde ein besonderes Augenmerk auf die breitgefächerte Expertise hinsichtlich des Betätigungsfelds und der konkret im Beruf betrachteten Aspekte von IT-Sicherheit gelegt: Zwei Start-up-Gründer, zwei Professoren der Informatik, ein IT-Sicherheitsbeauftragter aus dem Bankenbereich und auch zwei Führungskräfte von NGOs haben sich zu den Interviews bereit erklärt. Der Kontext, in dem sich die Spezialist*innen mit Fragestellungen der Informationssicherheit beschäftigen, ist entsprechend ihrer Professionen ebenso vielfältig und reicht von wissenschaftlichen Betrachtungen angewandter IT-Sicherheit über maschinelles Lernen, Banking und Web-Technologien bis hin zu gesellschaftlichen Auswirkungen der Informatik. Die Interviews werden explorativ geführt, den Expert*innen wird dabei entsprechend Forschungsfrage 1 lediglich eine vorgegebene Frage gestellt und anhand der Ausführungen ggf. weiter nachgefragt: „Welche Begriffe und Themen der IT-Sicherheit sind aus Ihrer Sicht für alle Menschen relevant?“. Anschließend werden die Interviews transkribiert und mithilfe der Qualitativen Inhaltsanalyse nach Mayring [Ma10] ausgewertet. Die Kodierung der Interviewtranskripte erfolgt dann in zwei Schritten: Zunächst werden die Äußerungen der Expert*innen pro Sinnabschnitt deduktiv einer der 19 „knowledge areas“ des CyBOKs [Ra18] zugeordnet. Pro „knowledge area“ werden die Ausführungen der Fachkräfte anschließend zu einem induktiv-generierten Kategoriensystem von Konzepten, Ideen und Begriffen qualitativ synthetisiert und kodiert (z. B. in Kategorien wie „Sicherheit als relativer Zustand“). Dies liefert die Anhaltspunkte zur Beantwortung der ersten Forschungsfrage.

Für die zweite Forschungsfrage wird ein Vergleich der relativen Anzahl der Expert*innen, die Äußerungen zu einer der 19 „knowledge areas“ tätigen, mit der relativen Anzahl, wie häufig diese „knowledge area“ in aktuellen nationalen und internationalen Curricula repräsentiert wird, durchgeführt: Der Kodiermodus ist binär („ja“, „nein“), so dass – wie auch in der herangezogenen Curricula-Analyse – bei Erwähnung eines Themas aus einer „knowledge area“ bereits eine „ja“-Kodierung stattfindet – unabhängig der Ausführlichkeit der Äußerungen zu diesem Thema.

4 Ergebnisse

4.1 Zentrale Themen aus Expertensicht

Eine kompakte Fassung der Ergebnisse zur ersten Forschungsfrage findet sich in Abb. 1. Im Folgenden sollen ergänzend dazu ausgewählte, in Curricula bisher nicht respräsentierte und besonders brisante Kernaussagen der Expert*innen nochmals pro „knowledge area“ bzw. „broader category“ illustriert werden.

CyBOK's Broader Categories	**CyBOK's Knowledge Areas**	Kernaussagen zu zentralen **Ideen und Konzepten**
Human, Organisational & Regulatory Aspects 	Risk Management & Governance	• **verschiedene Blickwinkel** auf Sicherheit • **Notwendigkeit des Abwägens**: • Sicherheit als **relativer Zustand** • Schutzziele im **Zielkonflikt** • Gefahr des **schwächsten Glieds** • **Erkennen** von Sicherheitsvorfällen
	Law & Regulation	• Auswirkungen auf alltägliche Leben
	Human Factors	• **Sicherheitsbewusstsein** als "mindset" und "culture" • gesellschaftliche **Auswirkungen** von Sicherheitsvorfällen • **"usability"** als Bestimmungsfaktor
	Privacy & Online Rights	• **Datenschutz** als technischer Schutz von Menschen (!) **vor Auswirkungen** von Datenverarbeitung • Schutz **durch Rechte** statt durch Regeln als **Bildungsansatz**
Attacks & Defences 	Adversarial Behaviours	• **technische vs. menschliche** Schwachstellen • Angreifer von außen vs. **Angreifer von innen**
	Incident Management	• Orientierung an Maßnahmen zur **Qualitätssicherung** • **Angriffsanalyse**
Systems Security 	Cryptography	• **Alice-Bob**-Szenario • **symmetrische vs. asymmetrische** Verschlüsselung • **Schlüsseltauschverfahren** • Auswirkungen des **Quantencomputings** • Hashfunktion, Digitale Signatur
	Distributed Systems Security	• Funktionsweise von **Cloud-Computing**
	Authentication & Authorisation	• **weltweit** eindeutige **Identifier**
Software Platform Security	**3 Areas:** SW Security / Web & Mobile Security / Secure SW Lifecycle	• technische **Grundlagen des Webs** • **Nutzerverfolgung** im Web • **Open Source** als Sicherheitskonzept für Software • Bedeutung rascher **Sicherheitsupdates**
Infrastructure Security	Network Security	• allgemeine **Kommunikationsabläufe** • Gefahren **drahtloser** Kommunikation
	Cyber Physical Systems	• Funktion & Schutz alltäglicher **IoT-Geräte**

Abb. 1: Kernaussagen der Expertinnen und Experten.

4.1.1 Themenfeld: Risk Management & Governance

Verschiedene Blickwinkel auf Sicherheit. Von großer Wichtigkeit stufte so ein Interviewpartner aus der Wissenschaft ein, unter welchen zwei verschiedenen Blickwinkeln der deutsche Begriff der „Sicherheit“ betrachtet werden kann. Im Englischen existieren für „Sicherheit“ zwei verschiedene Fachtermini, dies sind der Begriff der „safety“ und der „security“. Die „safety“ bezeichnet die funktionale Sicherheit eines IT-Systems, den Schutz der Umgebung vor dem System, und entspricht im Deutschen in etwa dem Begriff „Betriebssicherheit“. Beispielhaft für eine Fragestellung der „safety“ skizziert der Interviewpartner das Szenario eines selbstfahrenden Autos, das keinen (selbstverschuldeten) Unfall verursachen soll. Anders konzipiert ist hingegen die Vorstellung der „security“ als Schutz des IT-Systems vor Eingriffen von außerhalb: Sie entspricht im Deutschen ungefähr dem Begriff der „Angriffssicherheit“ bzw. „Schutz“ (beispielsweise vor Malware, Hackerangriffen usw.). So werde (umgangssprachlich) unter dem Terminus „IT-Sicherheit“ überwiegend also Sicherheit im Sinne der englischen „security“ verstanden. Im Bereich der „security“ seien die drei Schutzziele „Vertraulichkeit“ (engl. „confidentiality“), „Integrität“ (engl. „integrity“) und Zuverlässigkeit (engl. „availability“) grundlegend. Gegebenenfalls kann als viertes, gewissermaßen „orthogonales“ Schutzziel der Begriff der „privacy“ betrachtet werden.

Notwendigkeit des Abwägens und Sicherheit als relativer Zustand. Ein weiterer Experte aus der Wissenschaft führt folgende zwei Punkte für ein Verständnis von IT-Sicherheit an: 1. „Nichts ist sicher.“ 2. „Man muss es so sicher machen, dass potenzielle Angreifer kein Interesse mehr haben.“ Als analoges Beispiel veranschaulicht er: „Das kann man vergleichen mit einem Fahrradschloss: Ich muss nicht ein absolut sicheres Fahrradschloss haben, das kostet eine Million Euro – mein Fahrrad kostet aber gar nicht so viel. Ich brauche nur ein Fahrradschloss, das besser ist als die Fahrradschlösser um mich herum.“

Schutzziele im Zielkonflikt. Ein anderer Interviewter erweitert das Spannungsfeld konkurrierender Faktoren noch: „Es geht somit um den Zielkonflikt, den jeder Einzelne hat: Zuhause bleiben und nichts tun ist am sichersten.“ In Bezug auf die Wirtschaft stellt er folgenden Zielkonflikt dar: „Wie auch bei jeder Firma: Das Sicherste ist gar keine Anbindung von Computersystemen an die Außenwelt – dies ist jedoch nicht konkurrenzfähig!“

Gefahr des schwächsten Glieds. Wichtig sei für das Verständnis bezüglich Sicherheitskonzepten nach einer Fachkraft weiterhin die Problematik des schwächsten Glieds: „Man hat nicht immer ein klassisches Szenario vorliegen, wie, dass Sicherheitsvorfälle sich beim Vorliegen kryptographischer Schwächen ereignen – das ist eher selten der Fall. Meistens haben Sicherheitskonzepte per se eine Schwäche: Hier gilt es [für einen Angreifenden] das schwächste Element zu finden und dann zu überprüfen, ob es schwach genug ist.“

Erkennen von Sicherheitsvorfällen. Der Fall, dass keine „guten“ Sicherheitskonzepte eingesetzt werden (können) und welche Konsequenzen dies mit sich bringen kann, wie beispielsweise einen „Datendiebstahl“ (engl. „data breach“), ist für eine Fachperson

ebenso zentral: Hier können weitere Kontrollmaßnahmen (engl. „checks and balances“), insbesondere zur frühzeitigen Erkennung von Sicherheitsvorfällen, zur Security des Systems beitragen.

4.1.2 Themenfeld: Law & Regulation

Bezüglich der rechtlichen Situation wurde darauf hingewiesen, dass es mittlerweile gute internationale Standards im Bereich der IT-Sicherheit gebe. In Bezug auf die Frage, welche Gesetzgebungen wiederum für alle Menschen relevant sind, werden aber besonders Gesetzgebungen, die Auswirkungen auf das alltägliche Leben haben, wie die europäische eIDAS Verordnung (Onlinefunktion des Personalausweises) und die europäische Datenschutz-Grundverordnung (z. B. die verpflichtende Zustimmung zu Cookies) genannt.

4.1.3 Themenfeld: Human Factors

Informationssicherheitsbewusstsein. Für die Expert*innen ist hier der Gedanke eines Informationssicherheitsbewusstseins (engl. „security awareness“) fundamental. Betont wird insbesondere der Aspekt, dass dieses weit über ein rein kognitives Faktenwissen hinausgeht: „You can be documented, you can be fully compliant with certifications, but actually in the end . . . IT security, Information security is a culture. It’s an element of an organisational culture or individual for that matter. . . it is almost like a mindset.“ Im Unternehmenskontext bestehe für die IT-Sicherheitsbeauftragten eine absolute Notwendig- und Verantwortlichkeit, dieses Bewusstsein allen Menschen zu vermitteln. Anekdotisch wird hier von der IT-Abteilung einer Schweizer Bank berichtet, die, neben Schulungen im Bereich Sicherheit, ihren Mitarbeitenden von Zeit zu Zeit Phishing-E-Mails sendet, um das Bewusstsein ihrer Mitarbeiter in diesem Bereich zu überprüfen.

Usability als Bestimmungsfaktor. Als anspruchsvolle Fragestellung mit hohem Diskussionsbedarf wird auch betrachtet, wie IT in der Zukunft sicher und für alle Menschen einfach bedienbar gestaltet werden kann: Nutzer*innen sollen durch adäquate Konzepte und Tools unterstützt werden, Entscheidungen treffen zu können. Letztendlich müssten die User aber selbst sicherheitsbewusst handeln – vollständig kann ihnen diese Aufgabe von technischer Seite nicht abgenommen werden: „Machines can’t classify information as dangerous or not. It’s the human beings that interpret that data. You know, whether it is IT security, whether it is censorship, all these sort of topics. It’s the human perception of this, that is important.“

4.1.4 Themenfeld: Privacy & Online Rights

Datenschutz als technischer Schutz der Menschen vor Auswirkungen der Datenverarbeitung. In mehreren Interviews wird der Begriff „privacy“ als zentraler Begriff

genannt, wobei der deutsche Begriff „Datenschutz“ mitunter völlig anders konnotiert sei: Während man unter „Datenschutz“ im DACH-Raum vor allem der rechtliche Schutz von persönlichen Daten verstehe, so bedeute „privacy“ gerade auch den technischen (!) Schutz vor Datenverarbeitung. Darüber hinaus wird betont, dass die eigentliche Zielsetzung von „Datenschutz“ nicht so sehr das Schützen von Daten sei – als vielmehr die Menschen vor den Auswirkungen der Datenverarbeitung zu schützen. Als anschauliches Szenario führt eine Fachperson Folgendes an: „Sie suchen im Internet nach bestimmten Gesundheitsinformationen, weil Sie jetzt gerade einen Fachartikel oder für Ihre Arbeit recherchieren – und am nächsten Tag kündigt Ihnen Ihre Krankenversicherung, verdoppelt die Preise etc.“

Schutz durch Rechte statt durch Regeln als Bildungsansatz. Ebenso werden verschiedene Ansätze genannt, wie speziell im Bereich der „privacy“ versucht wurde und wird, Menschen zu schulen. Als Führungskraft einer NGO im Bereich digitaler Bildung verfügt hier eine der befragten Fachpersonen über tiefergehende Erfahrungen: Bis vor circa zehn Jahren sei vorwiegend der Ansatz verfolgt worden, Schüler*innen vor den Gefahren des Internets durch Auferlegung eines Regelwerks zu schützen („walled garden“, „protection-based approach“). Dieser Ansatz erwies sich jedoch nicht als nachhaltig, da die Jugendlichen derartige Regeln schlussendlich ignorierten. Heutzutage solle deshalb vornehmlich eine andere Strategie verfolgt werden: Den Schüler*innen solle geholfen werden, zu verstehen, wie die Technologie funktioniert, damit sie auf Grund dieses Wissens eigenständige Entscheidungen treffen können. Die Jugendlichen sollen somit verstehen, welche Wahl sie bezüglich der Weitergabe von privaten Daten in der Interaktion mit Technologien haben („rights-based approach“).

4.1.5 Themenfeld: Adversarial Behaviour

Technische vs. menschliche Schwachstellen. Von den Expert*innen werden potentielle Angreifende in zwei grobe Kategorien unterteilt, die sich durch die Art der Beschaffenheit des ausgenutzten Einfallstores unterscheiden: „There are broadly speaking two levels, if you want to think about security. First is technical, second is all about humans and how you can manipulate humans to do things.“

Angreifer von außen vs. Insider. Ein interviewter Spezialist hebt hervor, dass Angriffe – wie oft als erstes assoziiert – nicht nur von Dritten außerhalb eines Systems, eines Unternehmens unternommen werden, sondern teils auch von innen heraus erfolgen: „Zu Sicherheitsproblemen in Firmen, zu wirklichen ‚security breaches‘: Es ist häufig nicht so, wie man das aus dem Film kennt, dass ein Hacker draußen sitzt, programmiert und sich bemüht, durch eine Firewall einzubrechen, sondern ein Großteil der Angreifer kommt von innen. Dabei handelt es sich oft um eingeschleuste Sachen – z. B. durch übellaunige Mitarbeiter. Wenn man IT-Sicherheit nur als rein technisches Thema behandelt, ist das zu kurz gegriffen und trifft, so meine ich, wiederum auch nicht das, was in vielen Fällen passiert.“

4.1.6 Themenfeld: Web and Mobile Security

Technische Grundlagen & Nutzerverfolgung im Web. Knapp die Hälfte der Befragten stufen technische Grundlagen – wie beispielsweise das Internet und wie Smartphones funktionieren – als Basiswissen ein, um überhaupt Sicherheitsthemen in diesem Bereich erfassen zu können. Von gängigen Techniken, die von verschiedenen Akteuren eingesetzt werden, um in irgendeiner Art und Weise an Informationen zu gelangen, die nicht offen bzw. offensichtlich zugänglich sind und die ein User nicht unbedingt preisgeben möchte, sollten alle Menschen Kenntnis besitzen. Als solche Techniken werden hier „Tracking“, „Fingerprinting“ und „Cookies“ genannt. Ein Experte mahnt an, dass zwar aufgrund von EU-Verordnungen über die Verwendung von Cookies auf Webseiten aufgeklärt werden muss, dass allerdings die Kenntnis, wozu Cookies überhaupt eingesetzt werden, nur unzureichend in der Bevölkerung vorhanden sei.

Doppelte Bedeutung rascher Sicherheitsupdates. Ein anderer Experte betont, dass allen Benutzer*innen von Web- und mobilen Anwendungen die Wichtigkeit eines zügigen Aufspielens von Software-Updates bewusst sein sollte: Nicht nur, weil damit bekannte oder auch bereits von Hackern aktiv ausgenutzte Sicherheitslücken geschlossen werden, sondern ebenso, da Angreifern bisher unbekannte Schwachstellen, die in diesen Updates behoben werden, dadurch potentiell bekannt würden.

4.2 Vergleich von Expertensicht und Curricula

Die Gegenüberstellung zur zweiten Forschungsfrage der Repräsentation der „knowledge areas“ in den Curricula gegenüber der Abdeckung durch die Expert*innen findet sich in Abbildung 2: Exemplarisch wurden die K-12 Computer Science Standards und die Bildungsstandards der GI (für die Sekundarstufe I und II als eine Einheit betrachtet) dort ebenso aufgenommen. Besonders große Abweichungen (größer 33 %) zwischen dem relativen Anteil der Curricula und dem der Expert*innen, die das Themenfeld wenigstens erwähnen, sind ebenso durch Pfeile gekennzeichnet.

Es ergeben sich die folgenden Auffälligkeiten aus den Auswertungen:

- Die analysierten Curricula beschränken sich in ihrer Gesamtheit auf weniger Themenbereiche der IT-Sicherheit als die befragten Expert*innen.
- Starke Diskrepanzen sind in der relativen Abdeckung zu folgenden Themenfeldern zu beobachten: „Adversarial Behaviours“, „Human Factors” und das größere Themenbereich der ‚Software Platform Security‘ sind im Vergleich selten in Curricula anzutreffen. Die zwei letztgenannten werden sogar in keinem bzw. die “Human Factors” bisher lediglich in den K-12 Standards erwähnt.
- Im Vergleich zu den Curricula sprechen weniger Expert*innen die Themenbereiche „Privacy & Online Rights“ wie auch „Law & Regulation“ an.

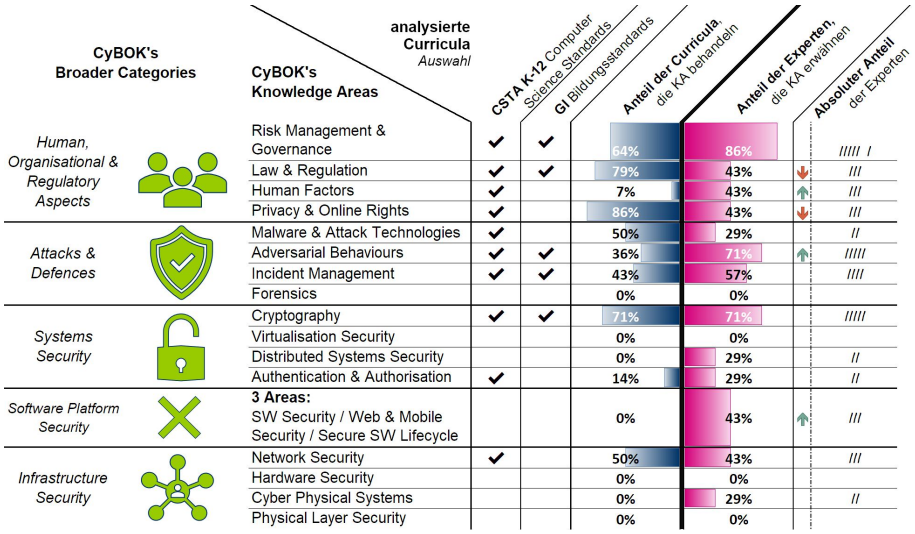

Abb. 2: Vergleich von Expertensicht mit den Curricula.

5 Diskussion

Die Studie unterlag verschiedenen Limitationen, insbesondere hinsichtlich der ersten Forschungsfrage muss hier nochmals die binäre Granularität des Kodiermodus angesprochen werden: Sowohl in der zugrunde liegenden Curriculums-Analyse als auch für die Interviews wurde hier beim Erwähnen von Themen innerhalb einer „knowledge area“ bereits als „vorhanden“ kodiert: Es steht die begründete Vermutung im Raum, dass viele Curricula etliche Themenbereiche der IT-Sicherheit nur relativ oberflächlich anschneiden, während die Expert*innen hier tiefer- und weiterführende Aspekte vorbringen. Insofern ist die in der Unterrichtspraxis relevante Lücke zwischen der curricularen Abdeckung an „knowledge areas“ und der der Spezialistinnen und Spezialisten noch größer anzunehmen, als dies Abb. 2 suggeriert. Die quantitative Auswertung des Expertenanteils in Abb. 2 kann zudem aufgrund der qualitativen Methodik nur als Indiz herangezogen werden.

Darüber hinaus ist eine (selbst-)kritische Expertenäußerung für die erste Forschungsfrage relevant: Eine Fachperson, die selbst etliche Begriffe und Konzepte der Kryptographie als für alle Menschen relevant deklarierte, gab abschließend zu bedenken, dass sie das Wissen darüber, wie Verschlüsselungsverfahren funktionieren, befürwortet, im späteren Leben das Wissen über die konkrete technische Umsetzung dieser Verfahren jedoch im Allgemeinen nicht von Bedeutung sei. Denkt man diese Überlegung weiter, könnte das bedeuten, dass weniger die konkrete Implementierung kryptographischer Verfahren im Schulunterricht, sondern mehr das Erkennen von Schwachstellen in Verfahren und das Weiterentwickeln dieser – für welche die Kryptographie einen möglichen Anwendungsfall darstellt – für die Expert*innen im Fokus stehen. Dies gilt es in weiterer Forschung zu

untersuchen. Auch eine Differenzierung zwischen Inhalten, die in der Schule, und solchen, die sinnvollerweise erst in der Berufsausbildung bzw. im Studium zu behandeln sind, ist durch weitere Forschungsarbeiten zu klären.

6 Fazit

Allgemeinbildender Informatikunterricht sollte sich bis zu einem gewissen Grad an der Praxis der Fachdisziplin orientieren und daher muss eingeordnet werden, welche Ideen, Konzepte und Begriffe der Fachpraxis eine allgemeinbildende Relevanz besitzen. Was diese Fragestellung betrifft, so divergieren in zentralen Bereichen der gegenwärtige Stand der Lehrpläne mit den von Expert*innen für wichtig befundenen Aspekten. Besonders die geringe – oder gar fehlende – Berücksichtigung der Themenfelder der „Human Factors“, der „Adversarial Behaviours“ und der „Web & Mobile Security“ in den Lehrplänen unterscheidet sich erheblich von der Einschätzung der befragten Expert*innen. Dabei erscheinen angesprochene Fragestellungen, wie „Wer ist überhaupt ein potentieller Angreifer, eine potentielle Angreiferin? Welche Motivation hat die Person?“, nicht nur fachlich grundlegend, sondern auch im Rahmen alltäglicher Handlungen, wie dem Administrieren des Heimnetzwerks oder der Wahl eines Passworts für einen Online-Dienst, relevant. Es besteht daher weiterer Forschungsbedarf, das Themenfeld der IT-Sicherheit im Informatikunterricht inhaltlich unter allgemeinbildenden Aspekten weiter didaktisch zu strukturieren und inhaltlich neu zu denken.

Literaturverzeichnis

[FB20] Furnell, Steven; Bishop, Matt: Addressing cyber security skills: the spectrum, not the silo. Computer Fraud & Security, 2020(2):6–11, 2020.

[Ma10] Mayring, Philipp: Qualitative Inhaltsanalyse. Grundlagen und Techniken. Beltz. Weinheim, 3:58, 2010.

[PHR20] Pencheva, Denny; Hallett, Joseph; Rashid, Awais: Bringing cyber to school: Integrating cybersecurity into secondary school education. IEEE Security & Privacy, 18(2):68–74, 2020.

[Ra18] Rashid, Awais; Danezis, George; Chivers, Howard; Lupu, Emil; Martin, Andrew; Lewis, Makayla; Peersman, Claudia: Scoping the cyber security body of knowledge. IEEE Security & Privacy, 16(3):96–102, 2018.

[RR20] Riel, Manuel; Romeike, Ralf: IT security in secondary CS education: is it missing in today's curricula? A qualitative comparison. In: Proceedings of the 15th Workshop on Primary and Secondary Computing Education. S. 1–2, 2020.