

9. September 2025 – Gemeinsame Erklärung von Forschenden zum neuen Vorschlag der EU-Präsidentschaft für die Verordnung über sexuellen Kindesmissbrauch

An:

Bundesministerium des Innern, Alexander Dobrindt

Bundesministerium der Justiz und für Verbraucherschutz, Stefanie Hubig

Bundesministerium für Digitales und Staatsmodernisierung, Karsten Wildberger

Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend, Karin Prien

Wir schreiben Ihnen als Reaktion auf den [neuen Vorschlag](#) der EU-Präsidentschaft vom 24. Juli 2025. Wir teilen Ihre Besorgnis über den sexuellen Missbrauch von Kindern und das damit verbundene Material (*Child sexual abuse material* - CSAM), das zu schweren Schäden für die Opfer und ihre Familien führt. In Anbetracht dessen begrüßen wir die Verbesserungen im neuen Entwurf des Verordnungsvorschlags, darunter die Aufnahme einiger Empfehlungen aus unseren Schreiben vom [Juli 2023](#), [Mai 2024](#) und [September 2024](#). Wir begrüßen insbesondere die Aufnahme von Bestimmungen, die die freiwillige Meldung illegaler Aktivitäten erleichtern, sowie die Verpflichtung, die Bearbeitung dieser Meldungen zu beschleunigen. Dies ist unerlässlich, um eine schnelle und wirksame Hilfe für Missbrauchsopfer zu gewährleisten.

Wir stellen jedoch mit Bestürzung fest, dass keine der Änderungen unsere zentralen Bedenken berücksichtigt: Es ist schlichtweg unmöglich, bekannte und neue Darstellungen des sexuellen Missbrauchs von Kindern für Hunderte Millionen Nutzerinnen und Nutzer mit einer akzeptablen Genauigkeit zu erkennen, unabhängig von der eingesetzten Filtertechnik. Darüber hinaus untergräbt eine Detektion direkt auf dem Gerät, unabhängig von ihrer technischen Umsetzung, von Natur aus den Schutz, den Ende-zu-Ende-Verschlüsselung eigentlich gewährleisten soll. Noch problematischer ist, dass die Änderungen im Vorschlag die Abhängigkeit von technischen Mitteln weiter verstärken. Dadurch verschärfen sich die Sicherheits- und Datenschutzrisiken für die Bevölkerung, ohne dass zugleich eine wirksame Verbesserung des Schutzes für Kinder garantiert ist. Wir gehen im Folgenden näher auf diese Punkte ein.

Der neue Vorschlag würde – ähnlich wie seine Vorgänger – beispiellose Möglichkeiten für Überwachung, Kontrolle und Zensur schaffen und birgt ein inhärentes Risiko für den Missbrauch durch weniger demokratische Regime. Das heute erreichte Sicherheits- und Datenschutzniveau in der digitalen Kommunikation und in IT-Systemen ist das Ergebnis jahrzehntelanger

gemeinsamer Anstrengungen von Forschung, Industrie und Politik. Es besteht kein Zweifel, dass dieser Vorschlag diese Sicherheits- und Datenschutzmaßnahmen, die für den Schutz der digitalen Gesellschaft unerlässlich sind, vollständig untergräbt.

Wir bedauern auch, dass es den politischen Entscheidungsträgerinnen und Entscheidungsträgern in den vergangenen zwei Jahren nicht gelungen ist, einen offenen Dialog mit Fachleuten zu diesem Thema zu führen. Trotz ernsthafter Zweifel an der Wirksamkeit von Detektionstechnologien gab es keine öffentliche Diskussion, Analyse und Bewertung dieser Technologien, die den Ansatz der vorgeschlagenen Verordnung rechtfertigen könnten. Dieser Mangel an Transparenz verhindert eine offene und fundierte Diskussion, in der geeignete Technologien zur Bekämpfung des Kindesmissbrauchs ermittelt werden könnten, und gefährdet zugleich die digitale Sicherheit unserer Gesellschaft in Europa und darüber hinaus.

1. Die Einschränkung des Erfassungsumfangs wird die Wirksamkeit nicht erhöhen.

Eine wesentliche Änderung, die vom Rat in Betracht gezogen wird, besteht darin, die geplante Detektion von CSAM (Child Sex and Abuse Material, Material über sexuellen Missbrauch von Kindern) auf **Bilder** (visuelle Informationen) und **URLs** zu beschränken. Dies steht im Gegensatz zu früheren Fassungen des Vorschlags, in denen die Detektion auf jegliches zwischen Nutzern versendete Material (einschließlich Text und Audio) angewendet werden sollte. Diese Änderung zielt darauf ab, den Anwendungsbereich des Vorschlags durch die Beschränkung auf bestimmte Dateiformate zu reduzieren, um die Verhältnismäßigkeit des Vorschlags im Hinblick auf die angestrebten Ziele zu erhöhen und Probleme im Zusammenhang mit der Erkennung illegaler Handlungen wie Grooming in Textform zu vermeiden.

Eine Reduzierung des Anwendungsbereichs ist zwar grundsätzlich zu begrüßen, beseitigt jedoch keines der in unseren früheren Schreiben geäußerten ernsthaften Bedenken. Es gibt keine wissenschaftliche Grundlage für die Behauptung, dass die Detektionstechnologie bei Bildern besser funktionieren würde als bei Textmaterial (weitere Einzelheiten finden Sie in [unserem ersten Offenen Brief](#)). Fachleute haben wiederholt gezeigt, dass Detektionsmethoden für bekannte Darstellungen des sexuellen Missbrauchs von Kindern leicht zu umgehen sind: Es reicht aus, einige Bits in einem Bild zu ändern, um sicherzustellen, dass ein Bild selbst aktuellste Detektionsmechanismen wirkungslos macht. Und obwohl es den Anschein haben mag, dass eine Geheimhaltung des Detektionsalgorithmus solche Umgehungen verhindern könnte, zeigen die neuesten Arbeiten zu diesem Thema, dass diese Art von Angriffen auch ohne Kenntnis des vom Detektionsmechanismus verwendeten Algorithmus wirksam sein kann. Daher werden diejenigen, die CSAM verbreiten wollen, diese Methoden bald anwenden und den Detektionsmechanismus vollständig umgehen. **Bestehende Forschungsergebnisse bestätigen**

zudem, dass selbst modernste Detektoren inakzeptabel hohe Raten an Fehlalarmen und Fehldetektionen erzeugen würden, wodurch sie für groß angelegte Detektionskampagnen im Umfang von Hunderten von Millionen von Nutzern, wie sie in der vorgeschlagenen Verordnung gefordert werden, ungeeignet sind.

Der aktuelle Vorschlag führt erneut die Möglichkeit ein, maschinelles Lernen und künstliche Intelligenz einzusetzen, um auch unbekannte CSAM-Bilder zu erkennen. Wir bekräftigen, dass es unseres Wissens nach keinen Algorithmus für maschinelles Lernen gibt, der eine solche Detektion ohne eine große Anzahl von Fehlern durchführen kann (z. B. ist es selbst für Menschen schwierig, zwischen CSAM-Material und einvernehmlichem Sexting von Teenagern zu unterscheiden). Darüber hinaus sind alle bekannten Algorithmen grundsätzlich anfällig für Umgehungen. Sobald eine verpflichtende Detektion eingeführt wird, ist zudem mit einer Vielzahl neuer Angriffe durch Personen zu rechnen, die illegales Material verbreiten wollen. **Angesichts der Tatsache, dass KI-basierte Technologien eine enorme Angriffsfläche bieten und es unmöglich ist, diese Angriffsfläche vollständig zu beseitigen, gehen wir davon aus, dass diese Technologien für die CSAM-Detektion höchst ineffektiv sein werden.**

Über visuelle Informationen hinaus sieht der neue Vorschlag zusätzlich die Überprüfung von URLs auf illegale Inhalte vor. Bei URLs ist eine Umgehung noch einfacher: Die Umleitung von URLs ist über kommerzielle Dienste oder lokal trivial umsetzbar und kann selbst von unerfahrenen Benutzern ohne Schwierigkeiten durchgeführt werden. Die Vielzahl der Möglichkeiten, URLs leicht zu ändern, macht die Detektion bösartiger URLs zu einem zentralen, aber ungelösten Problem der Websicherheit. Tatsächlich stehen wir vor ähnlichen Herausforderungen im Zusammenhang mit der Erkennung von Eindringlingen, der Identifizierung von Schadsoftware oder der Blockierung von Werbung. Obwohl dieses Problem von Industrie und Wissenschaft intensiv erforscht wird, ist es bekanntermaßen unlösbar. Deshalb verzichten Detektionssysteme bewusst darauf, URLs als primäre Entscheidungsgrundlage zu nutzen, um Manipulationen zu vermeiden, die die Wirksamkeit des Detektors beeinträchtigen. **Es gibt keinen Grund zu der Annahme, dass das Ergebnis bei URLs, die CSAM zugänglich machen, anders ausfallen würde als in anderen Bereichen, in denen bösartige URLs ebenfalls nicht zuverlässig identifiziert werden können.**

Intuitiv mag das Scannen von CSAM auf Endgeräten ähnlich wie die Prüfung von Schadsoftware durch Antivirensoftware erscheinen, aber diese beiden Probleme unterscheiden sich grundlegend. Die Erkennung von Schadsoftware funktioniert gut, wenn sie auf klare, genau definierte Bedrohungen abzielen kann, während die CSAM-Erkennung von Natur aus kontextabhängig ist und technisch nicht eindeutig definiert werden kann – zum Beispiel einvernehmliche Textnachrichten von Teenagern, medizinische Aufnahmen oder Bilder von Familienurlaube. Daher können CSAM-Detektoren grundsätzlich nicht mit der Zuverlässigkeit

von Schadsoftware-Scannern mithalten. Hinzu kommt: Wird auf einem Gerät potenzielle Schadsoftware gefunden, entscheidet stets die Nutzerin oder der Nutzer selbst über das weitere Vorgehen. Das heißt, dass Schadsoftware-Scans freiwillig, transparent und nicht an Hintertüren für Strafverfolgungsbehörden gebunden sind. Die Verpflichtung zum CSAM-Scannen auf dem Endgerät und die Bereitstellung des Zugriffs auf alle vom Algorithmus gefundenen Bilder für Strafverfolgungsbehörden ist mit all diesen grundlegenden Sicherheitsvorkehrungen unvereinbar.

Zusammenfassend lässt sich festhalten, dass die vorgeschlagenen Änderungen das Kernproblem nicht lösen: Die derzeit verfügbaren Detektionstechnologien sind weit davon entfernt, die im Zusammenhang mit dem CSA-Schutz erforderliche hohe Genauigkeit zu erreichen. Alle Sicherheits- und Datenschutzstudien in diesem Bereich deuten übereinstimmend darauf hin, dass die Probleme, die sie unzuverlässig machen, systemimmanent sind und auch in Zukunft nicht beseitigt werden können. **Es gibt also keinerlei Anhaltspunkte dafür, dass die im Vorschlag vorgesehenen Anpassungen beim Umfang der Erfassung und Detektion einen spürbaren Unterschied gegenüber früheren Entwürfen bewirken würden.**

2. Die Detektion auf dem Gerät hebt den Verschlüsselungsschutz von Natur aus auf

Der Vorschlag verlangt, dass die CSAM-Detektionstechnologie nicht zu einer „*Schwächung des durch Verschlüsselung gebotenen Schutzes*“ führen darf. Wir stimmen dieser Ansicht uneingeschränkt zu: End-to-End-Verschlüsselung (E2EE) ist unerlässlich, damit Bürgerinnen und Bürger aus der EU sicher und vertraulich online kommunizieren können, insbesondere wenn man bedenkt, dass zentrale Teile unserer Kommunikationsinfrastruktur von US-amerikanischen Big-Tech-Unternehmen kontrolliert werden und viele Nationalstaaten ihre Überwachungsmöglichkeiten sowohl [auf dem Gerät](#) als auch [während der Übertragung](#) erweitert haben. Verschlüsselung schützt dabei nicht nur die Zivilgesellschaft, sondern auch [EU-Politiker](#), **Entscheidungsträger, Strafverfolgungsbehörden und Verteidigungskräfte sind ebenfalls in hohem Maße auf E2E-Verschlüsselung angewiesen**, um eine sichere Kommunikation vor internen und externen Bedrohungen zu gewährleisten.

Es ist jedoch unmöglich, Material zu detektieren und entsprechende Berichte zu übermitteln, ohne die Verschlüsselung zu unterminieren. Zu den zentralen Gestaltungsprinzipien eines sicheren End-to-End-Verschlüsselungsschutzes gehören (i) die Gewährleistung, dass nur die beiden vorgesehenen Endpunkte auf die Daten zugreifen können, und (ii) die Vermeidung eines Single Point of Failures. Die Durchsetzung eines Detektionsmechanismus zum Scannen privater Daten vor ihrer Verschlüsselung – mit der Möglichkeit, sie nach der Überprüfung an die Strafverfolgungsbehörden zu übermitteln – verstößt von Natur aus gegen beide Grundsätze: **Sie**

untergräbt die zentrale Kerneigenschaft von E2EE, indem sie über den Detektionsmechanismus auf die privaten Daten zugreift, und schafft zugleich durch die erzwungene Detektion einen einzelnen Fehlerpunkt für alle sicheren E2E-Systeme.

Tatsächlich vergrößert der Detektionsmechanismus die Angriffsfläche erheblich und wird selbst zu einem hochsensiblen Ziel für Angreifer. Der Mechanismus kann technisch nicht auf die Detektion von CSAM oder die Erfassung visueller Informationen und URLs beschränkt werden. Es ist ein Leichtes, ihn so umzukonfigurieren, dass er andere Arten von Daten identifiziert und weitere Arten von Informationen erfasst, die mit anderen Straftaten oder finanziellen oder politischen Interessen in Zusammenhang stehen (z. B. Memes über politische Parteien). Darüber hinaus scheint die derzeitige Einschränkung des Anwendungsbereichs nur eine vorübergehende Beschwichtigung zu sein, und das [Änderungsprotokoll der vorgeschlagenen Verordnung \[in Bezug auf Grooming, S. 2, S. 4\]](#) deutet darauf hin, dass der Anwendungsbereich in Zukunft wieder auf Audio- und Textdaten ausgeweitet werden soll. Mit anderen Worten: **Der neue Vorschlag geht nicht auf unsere Bedenken hinsichtlich der möglichen Funktionsausweitung der geräteinternen Detektion ein.**

Der neue Vorschlag bekräftigt auch frühere Änderungen, mit denen der Anwendungsbereich der Detektion auf sogenannte „risikoreiche“ Teile oder Komponenten von Diensten beschränkt werden soll. **Die Definition von „risikoreich“ würde jedoch einige Dienste in ihrer Gesamtheit erfassen.** Ein herausragendes Beispiel sind E2E-verschlüsselte Messaging-Dienste wie Signal oder WhatsApp, die nicht nur von der breiten Bevölkerung, sondern auch von Politik, Medien, Menschenrechtsorganisationen, EU-Institutionen und Strafverfolgungsbehörden genutzt werden. Sollte der Vorschlag angenommen werden, würde der durch diese Apps gebotene Schutz wegfallen. Signal hat bereits angekündigt, seinen [Dienst in der EU einzustellen, sollte die geräteinterne Erkennung](#) verpflichtend werden, da jede Umsetzung zwangsläufig den Grundsatz der E2E-Verschlüsselung brechen und die Sicherheit der Nutzer gefährden würde.

Schließlich würde die Detektion eine Verarbeitung von Daten außerhalb des Geltungsbereichs der E2E-Verschlüsselung erfordern. Dies bedeutet, dass private Kommunikationsinhalte, die im Verdacht stehen, Darstellungen des sexuellen Missbrauchs von Kindern zu sein (was jedoch, wie in unserem ersten Punkt dargelegt, nicht garantiert ist), das Gerät des Nutzers verlassen und möglicherweise von nationalen Behörden abgerufen werden könnten. Dies entspricht dem Fall Podchasov gegen Russland, in dem der Europäische Gerichtshof für Menschenrechte erneut bekräftigte, dass bereits **die bloße Speicherung von Daten, die das Privatleben einer Person betreffen, einen Eingriff im Sinne von Artikel 8 (Recht auf Privatsphäre)** darstellt.

Zusammenfassend lässt sich sagen, dass die Auswirkungen des neuen Vorschlags eindeutig gegen die Grundprinzipien von Ende-zu-Ende-Verschlüsselung verstoßen und zu einer

Schwächung des durch Verschlüsselung gebotenen Schutzes führen werden. Darüber hinaus bedroht diese Schwächung unser Grundrecht auf Privatsphäre und kann schwerwiegende Folgen für unsere demokratischen Prozesse und die nationale Sicherheit haben, indem sie vertrauliche digitale Kommunikation verhindert.

3. Die Verpflichtung zur Anwendung aller möglichen technischen Schutzmaßnahmen erhöht nicht die Sicherheit

Eine weitere kritische Änderung im neuen Vorschlag besteht darin, dass Dienstleister verpflichtet werden, „**alle angemessenen Maßnahmen zu ergreifen, um das Risiko zu mindern, dass ihre Dienste missbraucht werden**“, und dass neue Bestimmungen zur Förderung und Regulierung der Anwendung von „*Maßnahmen zur Altersüberprüfung und Altersfeststellung*“ aufgenommen werden.

Zunächst möchten wir betonen, dass zusätzliche Maßnahmen im Bereich der Sicherheit nicht immer zu einem wirksameren Schutz führen. Im Gegenteil: Die Einführung neuer Maßnahmen könnte die erzielte Sicherheit des Systems auf das Niveau der schwächsten Schutzmaßnahme reduzieren und gleichzeitig die Komplexität – und damit auch die Risiken – für das Gesamtsystem erhöhen. Im Falle dieses Vorschlags kann die Einführung weiterer Schutzmaßnahmen angesichts der Unzulänglichkeit der Detektionstechnologien, wie im vorigen Punkt erläutert, nur wenig zusätzlichen effektiven Schutz für Nutzende und Opfer bringen.

Darüber hinaus sind wir nicht davon überzeugt, dass die Verpflichtung zur Altersüberprüfung für den Zugriff auf Inhalte im Internet die gewünschten Vorteile bringt. Erstens können Altersüberprüfungen leicht umgangen werden. Wir haben dies in Großbritannien beobachtet, wo die Umsetzung des *Online Safety Acts* dazu führte, dass Nutzende auf Dienste ausweichen, die keine Kontrollen durchführen – was immer dann der Fall sein wird, solange es Dienste gibt, die keine Kontrollen durchführen. In Großbritannien wurde auch ein Anstieg der VPN-Verbindungen beobachtet, um die Überprüfung durch den Zugriff auf Server von anderen Standorten aus zu umgehen. Darüber hinaus führt dies zu neuen Risiken. Der obligatorische Charakter der Altersüberprüfung kann zu einem Grund werden, die Nutzung von Datenschutztechnologien wie VPNs zu verbieten, die zur Umgehung dieser Überprüfung beitragen können. Dies würde die Meinungs- und Informationsfreiheit gefährden, indem es die private Internetnutzung einschränkt, und es würde zentrale Werkzeuge untergraben, auf die Whistleblower, Medienschaffende und Menschenrechtsorganisationen angewiesen sind. Darüber hinaus hätte ein solcher Schritt gravierende Folgen für die Internetsicherheit, da VPNs für die Industrie eine wesentliche Grundlage darstellen, um interne und externe Remote-Dienste sicher nutzen zu können.

Zweitens: Selbst wenn die Altersüberprüfung mit überprüfbaren und zertifizierten Attributen durchgeführt wird, wie etwa in der neuen Altersüberprüfungs-App der EU, untergräbt sie dennoch die Grundprinzipien der Online-Anonymität und des offenen Zugangs zu Informationen. Zunächst wird eine solche Technologie vielleicht nur verlangt, um nachzuweisen, dass man älter als 18 Jahre ist. Sobald sie eingeführt ist, kann dieselbe Technologie dazu verwendet werden, die Offenlegung anderer und identifizierenden Informationen wie Geschlecht, Nationalität oder Gesundheitszustand zu verlangen. Vor ihrer Einführung muss daher klar nachgewiesen werden, dass die Einführung einer solchen Technologie tatsächlich die gewünschten Vorteile mit sich bringen würde, sowie Belege dafür, dass die damit verbundenen Nachteile (z. B. die Möglichkeit der Nachverfolgung oder Zensur) wirksam verhindert werden können.

Zudem befürchten wir, dass der plötzliche Druck, solche Lösungen zu implementieren, zu übereilten Entscheidungen führen könnte. Erste Prototypen einiger Big-Tech-Anbieter wurden nicht eingehend untersucht und es fehlt eine offene Begutachtung durch unabhängige Fachleute. Ihre Verwendung würde nicht nur ein Risiko in Bezug auf die Leistung mit sich bringen, sondern auch eine kritische Abhängigkeit Europas von Big Tech in einer zentralen Infrastruktur zum Schutz von Kindern schaffen.

Wir kommen zu dem Schluss, dass eine Erhöhung der Anzahl an Technologien, die zur Bekämpfung des Problems des sexuellen Missbrauchs von Kindern eingesetzt werden sollen, und deren obligatorische Einführung nicht nur *keine* Verbesserung gegenüber dem vorherigen Vorschlag darstellen, sondern **die Probleme noch verstärken und die potenziellen negativen Auswirkungen dieser vorgeschlagenen Verordnung auf die Sicherheit des Internets und die Freiheit und Privatsphäre seiner Nutzer** noch vergrößern.

4. Sichere Wege für den Kinderschutz

Zwei Jahre nach unserem ersten Schreiben möchten wir erneut betonen, dass angesichts der Grenzen der Technologie der derzeitige technologieorientierte Vorschlag, dessen Schwerpunkt auf der Entfernung von missbräuchlichem Material aus dem Internet auf Kosten der Kommunikationssicherheit liegt, nur wenig Potenzial hat, den Missbrauch an Kindern wirksam zu bekämpfen.

Wir erinnern daran, dass CSAM-Inhalte stets das Ergebnis von sexuellem Kindesmissbrauch sind. Ihre Beseitigung setzt daher die Bekämpfung des Missbrauchs selbst voraus, nicht alleine die Verhinderung der digitalen Verbreitung von Missbrauchsmaterial. Anstatt weiterhin auf Technologien mit zweifelhafter Wirksamkeit wie CSAM-Detektionsalgorithmen und

Altersüberprüfungen zu setzen, die die Sicherheit und Privatsphäre erheblich beeinträchtigen, möchten wir erneut auf die von Organisationen wie den Vereinten Nationen empfohlenen Maßnahmen aufmerksam machen. Dazu gehören Aufklärung (über Einwilligung, Normen und Werte, digitale Kompetenz und Online-Sicherheit sowie umfassende Sexualaufklärung), traumasensible Hotlines für Meldungen und keyword-basierte Interventionen.

Die Schritte hin zu einer besseren Meldung und schnelleren Entfernung von Inhalten sind wichtige Fortschritte, aber wir wiederholen unsere Empfehlung, die Investitionen und Anstrengungen zur Unterstützung bewährter Ansätze zur Beseitigung von Missbrauch erheblich zu erhöhen. Wird der Missbrauch selbst wirksam verhindert, verschwindet auch das missbräuchliche Material, ohne die sichere digitale Interaktion zu gefährden, die für die Sicherheit der Kinder, die die vorgeschlagene Verordnung schützen soll, unerlässlich ist.

Unterzeichnende in Deutschland:

Prof. Dr. Yasemin Acar	Paderborn University
Dr. Dirk Achenbach	FZI Research Center for Information Technology
Prof. Dr. Florian Adamsky	Hof University of Applied Sciences
Prof. Dr. Suzana Alpsancar	Paderborn University
Dr.-Ing. Ingmar Baumgart	FZI Research Center for Information Technology
Prof. Dr. Thomas Bayer	Ravensburg-Weingarten University of Applied Sciences
Dr. Steffen Becker	Ruhr University Bochum
Prof. Sebastian Berndt	Technische Hochschule Luebeck
Wasilij Beskorovajnov	FZI Research Center for Computer Science
Dr. Asia Biega	Max Planck Institute for Security and Privacy
Dr. Nina Bindel	MTG AG
Dr.-Ing. Roland Bless	Karlsruhe Institute of Technology
Prof. Dr. Kevin Borgolte	Ruhr University Bochum

Prof. Dr. Frank Breiting	Universität Augsburg
Dr. Sven Bugiel	CISPA Helmholtz Center for Information Security
Dr. Felix Butz	Humboldt University of Berlin
Prof. Chitchanok Chuengsatiansup	Hasso-Plattner-Institute, University of Potsdam
Prof. Jiska Classen	Hasso-Plattner-Institute, University of Potsdam
Prof. Dr. Cas Cremers	CISPA Helmholtz Center for Information Security
Dr. Daniel Demmler	Zama
Prof. Dr. Alexandra Dmitrienko	University of Wuerzburg
Prof. Dr. Martin Doll	Düsseldorf University of Applied Sciences
Prof. Dr. Derek Dreyer	Max Planck Institute for Software Systems
Prof. Dr. Sabine Döring	University of Tübingen
Prof. Dr. Kai Eckert	TH Mannheim
Dr. Kasma Edalatnejad	TU Darmstadt
Prof. Dr.-Ing. Thomas Eisenbarth	University of Lübeck
Dr.-Ing. Matthes Elstermann	University of Münster
Dr. Christina Ertural	Personal capacity
Prof. Matthias Faes	TU Dortmund
Prof. Sascha Fahl	CISPA Helmholtz Center for Information Security
Dr.-Ing. Aurore Fass	CISPA Helmholtz Center for Information Security
Prof. Sebastian Faust	TU Darmstadt
Prof. Dr. Hannes Federrath	University of Hamburg
Prof. Bernd Finkbeiner	CISPA Helmholtz Center for Information Security
Prof. Dr. Felix Freiling	FAU Erlangen-Nürnberg

Dr. Simon Friedberger	Mozilla
Prof. Florian Gallwitz	TH Nuremberg
Prof. Dr. Deepak Garg	Max Planck Institute for Software Systems
Dr. Evangelos Gazis	Huawei Technologies GmbH
Dr.-Ing. Kai Gellert	University of Wuppertal
Dr. Noemi Glaeser	Personal capacity
Dr. Maximilian Golla	CISPA Helmholtz Center for Information Security
Dr.-Ing. Marc Gourjon	Max Planck Institute for Security and Privacy
Prof. Dr.-Ing. Martin Grothe	Niederrhein University of Applied Sciences
Prof. Krishna P. Gummadi	Max Planck Institute for Software Systems
Prof. Dr.-Ing. Tim Güneysu	Ruhr University Bochum
Dr.-Ing. Tobias Handirk	genua GmbH
Dr.-Ing. Dominik Helm	TU Dortmund
Prof. Dr. Dominik Herrmann	University of Bamberg
Dr. Thomas Herzog	OWASP
Dr.-Ing. Jonas Hielscher	CISPA Helmholtz Center for Information Security
Prof. Matthias Hollick	TU Darmstadt
Prof. Thorsten Holz	Max Planck Institute for Security and Privacy
Prof. Dr. Ralph Holz	University of Münster
Dr. Máté Horváth	University of Wuppertal
Dr. Henry Hosseini	Westphalian University of Applied Sciences, University of Münster
Apl. Prof. Dr. Catalin Hritcu	Max Planck Institute for Security and Privacy
Dr. Katharina Huesmann	University of Münster
Prof. Dr. Martin Huesmann	University of Münster

Prof. Dr.-Ing. Luigi Lo Iacono	University of Giessen
Dr. Swen Jacobs	CISPA Helmholtz Center for Information Security
Prof. Dr.-Ing. Tibor Jager	University of Wuppertal
Prof. Dr. Martin Johns	TU Braunschweig
Prof. Ghassan Karame	Ruhr University Bochum
Prof. Dr. Stefan Katzenbeisser	University of Passau
Dr. Franziskus Kiefer	Cryspen
Prof. Dr. Eike Kiltz	Ruhr University Bochum
Dr. Attila Kinali	Max Planck Institute for Informatics
Dr. Ilya Kizhvatov	Personal capacity
Dr. Michael Klooß	Karlsruhe Institute of Technology
Dr. Konrad Kohbrok	Phoenix R&D
Dr. Katharina Krombholz	CISPA Helmholtz Center for Information Security
Prof. Dr. Klaas Ole Kuertz	Kiel University of Applied Sciences
Prof. Dr.-Ing. Andreas Kurtz	Heilbronn University of Applied Sciences
Dr. Robert Künnemann	CISPA Helmholtz Center for Information Security
Prof. Dr. Anja Lehmann	Hasso-Plattner-Institute, University of Potsdam
Dr. Wouter Lueks	CISPA Helmholtz Center for Information Security
Dr. Lin Lyu	University of Wuppertal
Prof. Dr. Klaus-Peter Lühr	Personal capacity
Prof. Dr.-Ing. Andreas Maier	FAU Erlangen-Nürnberg
Prof. Dr. Christian Mainka	University of Wuppertal
Dr. Kajetan Maliszewski	BIFOLD, TU Berlin
Prof. Dr. Karola Marky	Ruhr University Bochum
Ninja Marnau	CISPA Helmholtz Center for Information Security

Dr. Adrian Marotzke	Personal capacity
Prof. Dr.-Ing. Andreas Mayer	Heilbronn University of Applied Sciences
Dr. Jeremias Mechler	Karlsruhe Institute of Technology
Dr. Abraham Mhaidli	Max Planck Institute for Security and Privacy
Prof. Dr.-Ing. Markus Miettinen	Frankfurt University of Applied Sciences
Prof. Dr. Esfandiar Mohammadi	University of Lübeck
Prof. Dr. Veelasha Moonsamy	Ruhr University Bochum
Prof. Amir Moradi	TU Darmstadt
Dr. Christian Mouchet	Hasso-Plattner-Institute, University of Potsdam
Dr. Simon Oberthür	Paderborn University, SICP
Dr. Johannes Ottenhues	Karlsruhe Institute of Technology
Prof. Dr. Rebekah Overdorf	Ruhr University Bochum
Dr. Kentrell Owens	Max Planck Institute for Security and Privacy
Prof. Christof Paar	Max Planck Institute for Security and Privacy
Prof. Dr. Lorenz Panny	Technische Universität München
Dr. Sebastian Pape	Social Engineering Academy GmbH
Dr. Giancarlo Pellegrino	CISPA Helmholtz Center for Information Security
Dr. Maximilian Petras	HSU Hamburg
Prof. Dr. Joachim Posegga	University of Passau
Prof. Dr. Key Pousttchi	wi-mobile Institute for Digital Transformation
Dr. Daniela Pöhn	Universität der Bundeswehr München
Dr. Willy Quach	CISPA Helmholtz Center for Information Security
Prof. Dr. Kai Rannenberg	Goethe University Frankfurt
Dr. Stephan Rave	University of Münster

Prof. Dr. Dr. Christian Reuter	TU Darmstadt
Prof. Dr. Konrad Rieck	BIFOLD & TU Berlin
Dr. Doreen Riepel	CISPA Helmholtz Center for Information Security
Prof. Dr. Christian Riess	FAU Erlangen-Nürnberg
Prof. Dr. Stefanie Roos	University of Kaiserslautern-Landau
Prof. Christian Rossow	CISPA Helmholtz Center for Information Security
Prof. Paul Rösler	FAU Erlangen-Nürnberg
Prof. Dr. Christoph Saatjohann	University of Applied Sciences Münster
Prof. Dr. M. Angela Sasse	Ruhr University Bochum
Dr. Sajin Sasy	CISPA Helmholtz Center for Information Security
Dr. Jens Schade	TU Dresden
Dr. Martin Schanzenbach	Fraunhofer Institute for Applied and Integrated Security
Dr. Tim Schatto-Eckrodt	Hamburg University
Prof. Dr. Sebastian Schinzel	FH Münster, Fraunhofer SIT, Athene National Research Center for Applied Cybersecurity
Prof. Thomas Schneider	TU Darmstadt
Dr. Clara Schneidewind	Max Planck Institute for Security and Privacy
Peter Schoo	Personal capacity
Prof. Dr. Falk Schreiber	University of Konstanz
Dr. Moritz Schubotz	FIZ Karlsruhe
Prof. Dr. Stephan Schulz	DHBW Stuttgart
Dr. Matthias Schunter	Intel Labs
Prof. Dr. Peter Schwabe	Max Planck Institute for Security and Privacy, Radboud University
Prof. Jörg Schwenk	Ruhr University Bochum
Dr. Lea Schönherr	CISPA Helmholtz Center for Information Security

Dr. Johannes Schönrich-Sedlmeir	University of Münster
Dr. Henning Seidler	TU Berlin
Prof. Dr. Daniel Slamanig	Universität der Bundeswehr München
Prof. Dr.-Ing. Juraj Somorovsky	Paderborn University
Prof. Dr. Christoph Sorge	Saarland University
Dr. Aleksandra Sowa	FG PET, GI e.V.
Prof. Dr. Indra Spiecker	University of Cologne
Prof. Dr. Barbara Sprick	Technische Hochschule Aschaffenburg
Prof. Dr. Alexander Steen	University of Greifswald
Dr.-Ing. Ben Stock	CISPA Helmholtz Center for Information Security
Prof. Dr.-Ing. Thorsten Strufe	Karlsruhe Institute of Technology
Dr.-Ing. Philipp Terhoerst	Paderborn University
Prof. Kirsten Thommes	Paderborn University
Dr. Nils Ole Tippenhauer	CISPA Helmholtz Center for Information Security
Dr.-Ing. Amos Treiber	Personal Capacity
Prof. Carmela Troncoso	Max Planck Institute for Security and Privacy, EPFL
Prof. Dr. Florian Tschorsch	TU Dresden
Prof. Dr. Dominique Unruh	RWTH Aachen University
Prof. Dr. Tobias Urban	Westphalian University of Applied Sciences
Dr. Anjo Vahldiek-Oberwagner	Personal capacity
Dr. Marloes Venema	University of Wuppertal
Dr. Vasilis Ververis	Hasso-Plattner-Institute, University of Potsdam
Prof. Jilles Vreeken	CISPA Helmholtz Center for Information Security

Dr. Théophile Wallez	CISPA Helmholtz Center for Information Security
Dr. Valentin Weber	German Council on Foreign Relations
Prof. Dr. Andreas Westfeld	HTW Dresden
Dr.-Ing. Jan Wichelmann	Universität zu Lübeck
York Yannikos	Fraunhofer Institute for Secure Information Technology, ATHENE National Research Center for Applied Cybersecurity
Prof. Dr. Yuval Yarom	Ruhr University Bochum
Dr. Alexandros Zacharakis	Hasso-Plattner-Institute, University of Potsdam
Prof. Andreas Zeller	CISPA Helmholtz Center for Information Security
Dr. Xiao Zhang	CISPA Helmholtz Center for Information Security
Prof. Michael Zohner	Hochschule Fulda
Dr. Yixin Zou	Max Planck Institute for Security and Privacy

Weitere Unterzeichnende

Australia

Dr. Erik Buchholz	University of New South Wales
Prof. Qiang Tang	The University of Sydney
Prof. Vanessa Teague	Thinking Cybersecurity Pty Ltd, Australian National University

Austria

Prof. Dr. Elena Andreeva	TU Wien
Prof. Maria Eichlseder	Graz University of Technology

Prof. Dr. Juergen Fuss	University of Applied Sciences Upper Austria
Prof. Daniel Gruss	Graz University of Technology
Dr. Walter Hötendorfer	Research Institute – Digital Human Rights Center
Dr. Christoph Kerschbaumer	Mozilla
Dr. Stephan Krenn	Personal capacity
Prof. Martina Lindorfer	TU Wien
Dr. Thomas Loruenser	Austrian Institute of Technology
Univ.-Prof. Dr. Matteo Maffei	TU Wien
Univ.-Prof. Dr. Stefan Mangard	Graz University of Technology
Prof. René Mayrhofer	Johannes Kepler University Linz
Dr. Stefan More	Graz University of Technology
Univ.-Prof. Dr.-Ing. Frank Pallas	Salzburg University
Prof. Krzysztof Pietrzak	Institute of Science and Technology Austria
Dr. Sebastian Ramacher	Personal capacity
Univ.-Prof. Dr. Christian Rechberger	Graz University of Technology
Dr. Michael Roland	Johannes Kepler University Linz
Prof. Sujoy Sinha Roy	Graz University of Technology
Prof. Dr. Arnab Roy	University of Innsbruck
Dr. Johannes Sametinger	Johannes Kepler University Linz
Dr. Diogo Sasdelli	Universität für Weiterbildung Krems
Prof. Dr. Peter Schartner	Klagenfurt University
Univ.-Prof. Dr. Dominique Schröder	TU Wien
Prof. Mag. Dr. Wieland Schwinger	Johannes Kepler University Linz

Marek Sefranek	TU Wien
Prof. Dimitris Simos	University of Salzburg & FH Salzburg
Ing. Dr.iur. Christof Tschohl	Research Institute – Digital Human Rights Center
Prof. Edgar Weippl	University of Vienna

Belgium

Dr. Aysajan Abidin	KU Leuven
Dr. Shahla Atapoor	KU Leuven
Dr. Karim Baghery	KU Leuven
Dr. Eduard Baranov	UCLouvain
Dr. Emad Heydari Beni	KU Leuven
Robin Berjon	Supramundane Agency, Future of Technology Institute
Prof. Tijl De Bie	Ghent University
Dr. Marton Bognar	KU Leuven
Dr. Rosamunde Van Brakel	Vrije Universiteit Brussel
Prof. Antoon Bronselaer	Ghent University
Dr. Gaetan Cassiers	UCLouvain
Dr. Wouter Castryck	KU Leuven
Prof. Quentin De Coninck	UMONS
Prof. Bart Coppens	Ghent University
Prof. Geert Deconinck	KU Leuven
Dr. Thomas Decru	KU Leuven
Dr. Pierre Dewitte	KU Leuven
Prof. Claudia Diaz	KU Leuven
Prof. Laura Drechsler	KU Leuven/State Archives of Belgium/Open Universiteit

Prof. Jean-Michel Dricot	Université Libre de Bruxelles
Dr. Gertjan Franken	KU Leuven
Prof. Dr. Gloria Gonzalez Fuster	Vrije Universiteit Brussel
Dr. Mariana Gama	KU Leuven
Dr. Benedikt Gierlichs	KU Leuven
Dr. Milos Grujic	KU Leuven
Dr. Iness Ben Guirat	Université Libre de Bruxelles
Prof. Paul De Hert	Vrije Universiteit Brussel
Dr. Robin Jadoul	3MI Labs
Dr. Ir. Kristof Jannes	KU Leuven
Dr. Francois Koeune	UCLouvain
Prof. Dimitri Van Landuyt	KU Leuven
Dr. Ing. Jorn Lapon	KU Leuven
Dr. Diane Leblanc-Albarel	KU Leuven
Dr. Barry van Leeuwen	KU Leuven
Prof. Gregory Lewkowicz	Université Libre de Bruxelles
Dr. Mairon Mahzoun	3MI Labs, Eindhoven University of Technology
Dr. Hannes Mareen	Ghent University, imec
Dr. Ingrida Milkaite	Vrije Universiteit Brussel
Dr. Thorben Moos	UCLouvain
Prof. Yves Moreau	KU Leuven
Prof. Jan Tobias Muehlberg	Universite Libre de Bruxelles
Dr. Svetla Nikova	KU Leuven
Dr. Charles-Henry Bertrand Van Ouytsel	UCLouvain

Dr. Roel Peeters	KU Leuven
Prof. Olivier Pereira	UCLouvain
Prof. Thomas Peters	UCLouvain & FNRS
Prof. Jo Pierson	Hasselt University
Prof. Bart Preneel	KU Leuven
Dr. Frederik Questier	Vrije Universiteit Brussel
Prof. Jean-Jacques Quisquater	UCLouvain
Dr. Krijn Reijnders	KU Leuven
Mr. Sam van Rijn	PXL University of Applied Sciences and Arts
Dr. Vera Rimmer	KU Leuven
Prof. Etienne Riviere	UCLouvain
Prof. Florentin Rochet	UNamur
Prof. Sofie Royer	KU Leuven and ULiège
Dr. Enrique Argones Rúa	KU Leuven
Prof. Yvan Saeys	Ghent University
Prof. Wim Schoutens	KU Leuven
Prof. Laurent Schumacher	UNamur
Dr. ing. Merlijn Sebrechts	Ghent University, imec
Dr. Mahdi Sedaghat	Soundness Labs, KU Leuven
Prof. Dr. Dave Singelee	KU Leuven
Prof. Nigel Smart	KU Leuven, Zama
Prof. François-Xavier Standaert	UCLouvain
Prof. Dr. Janwillem Swalens	Vrije Universiteit Brussel
Prof. Mathy Vanhoef	KU Leuven

Prof. Dr. Ir. Ingrid Verbauwheide	KU Leuven
Dr. Rafael Gálvez Vizcaíno	KU Leuven
Dr. Iwein Vranckx	Engilico Engineering
Dr. Lennert Wouters	KU Leuven
Dr. Takahito Yoshizawa	KU Leuven

Bulgaria

Prof. Tsonka Baicheva	Bulgarian Academy of Sciences
Dr. Vesselin Bontchev	Bulgarian Academy of Sciences

Canada

Prof. Ian Goldberg	University of Waterloo
Dr. Ryan Henry	University of Calgary
Prof. Bailey Kacsmar	University of Alberta
Prof. Nicolas Papernot	University of Toronto and Vector Institute
Prof. David Murkami Wood	University of Ottawa

Croatia

Prof. Ante Derek	University of Zagreb
Prof. Marko Horvat	University of Zagreb
Prof. Tajana Ban Kirigin	University of Rijeka
Prof. Stjepan Picek	University of Zagreb, Radboud University

Cyprus

Prof. Elias Athanasopoulos University of Cyprus

Czechia

Prof. Petr Svenda, Ph.D. Masaryk University

Prof. Jan Hajny Brno University of Technology

Dr. Pavel Hubacek Czech Academy of Sciences, Charles University

Prof. Lukas Malina Brno University of Technology

Prof. Kamil Malinka Brno University of Technology

Prof. Vashek Matyas Masaryk University

Denmark

Prof. Diego F. Aranha Aarhus University

Prof. Aslan Askarov Aarhus University

Prof. Carsten Baum Technical University of Denmark

Dr. Stein Arne Brekke University of Copenhagen

Prof. Ivan Damgård Aarhus University

Prof. Dr. Holger Dell IT University of Copenhagen

Prof. Nicola Dragoni Technical University of Denmark

Prof. Andrzej Filinski University of Copenhagen

Prof. Rosario Giustolisi IT University of Copenhagen

Prof. Carla F. Griggio Aalborg University

Prof. Thore Husfeldt IT University of Copenhagen

Prof. Robin Kaarsgaard University of Southern Denmark

Prof. Lars Ramkilde Knudsen University of Southern Denmark

Prof. Christian Majenz Technical University of Denmark

Dr. Mikkel Kragh Mathiesen	University of Copenhagen
Prof. Jacopo Mauro	University of Southern Denmark
Prof. Peter Mayer	University of Southern Denmark
Prof. Hiraku Morita	University of Southern Denmark
Prof. Boel Nelson	University of Copenhagen
Prof. Ruben Niederhagen	University of Southern Denmark
Prof. Rasmus Løvenstein Olsen	Aalborg University
Prof. Claudio Orlandi	Aarhus University
Prof. Rasmus Pagh	University of Copenhagen
Prof. Jens Myrup Pedersen	Aalborg University
Prof. Peter Scholl	Aarhus University
Prof. Robin Sharp	Technical University of Denmark
Dr. Mark Simkin	Aarhus University
Prof. Luisa Siniscalchi	Technical University of Denmark
Prof. Lene Sorensen	Aalborg University
Assoc. Prof. Henning Thomsen	Aalborg University
Prof. Tyge Tiessen	Technical University of Denmark
Prof. Emmanouil Vasilomanolakis	Technical University of Denmark
Prof. Sophia Yakoubov	Aarhus University

Estonia

Dr. Sedat Akleylek	University of Tartu
Dr. Dan Bogdanov	Estonian Academy of Sciences

Dr. Maiara F. Bollauf	University of Tartu
Dr. Lukáš Daubner	University of Tartu
Dr. Ljubov Jaanuska	University of Tartu
Prof. Heiki-Jaan Kaalep	University of Tartu
Dr. Liina Kamm	Cybernetica AS
Dr. Ivan Koppel	University of Tartu
Dr. Toomas Krips	University of Tartu
Prof. Helger Lipmaa	University of Tartu
Dr. Chad Nester	University of Tartu
Dr. Arnis Parsovs	University of Tartu
Dr. Janno Siim	University of Tartu

Finland

Prof. Dr. Chris Brzuska	Aalto University
Prof. Kimmo Halunen	University of Oulu
Dr. Mikko Heikkilä	University of Helsinki
Prof. Camilla Hollanti	Aalto University
Prof. Antti Honkela	University of Helsinki
Prof. Mikko Kivelä	Aalto University
Prof. Dr. Russell W. F. Lai	Aalto University
Prof. Markku-Juhani O. Saarinen	Tampere University

France

Dr. Alexandre Hannud Abdo	CNRS
---------------------------	------

Dr. Marianne Akian	Inria
Prof. Gildas Avoine	INSA Rennes
Prof. David Baelde	Université de Rennes
Dr. Gustavo Banegas	Inria
Dr. Martin Bodin	Inria
Dr. Xavier Bonnetain	Inria
Dr. Daniel De Almeida Braga	Université de Rennes
Dr. Anne Canteaut	Inria
Dr. Riccardo Cappuzzo	Inria
Prof. Rémi Cogranne	Troyes University of Technology
Dr. Veronique Cortier	CNRS
Dr. Alexandre Debant	Inria
Dr. Stéphanie Delaune	CNRS
Dr. Jannik Dreier	Université de Lorraine
Dr. Sébastien Duval	Université de Lorraine
Dr. Benjamin Farinier	Université de Rennes
Dr. Barbara Fila	INSA Rennes
Dr. Caroline Fontaine	CNRS
Aurélien Francillon	EURECOM
Dr. Aymeric Fromherz	Inria
Prof. Joaquin Garcia-Alfaro	Institut Polytechnique de Paris
Dr. Pierrick Gaudry	CNRS
Prof. Louis Goubin	Versailles St-Quentin-en-Yvelines University
Dr. Cédric HERPSON	Sorbonne Université
Dr. Lucca Hirschi	Inria

Dr. Georgy Ishmaev	Inria
Dr. Charlie Jacomme	Inria
Dr. Adrien Koutsos	Inria
Dr. Steve Kremer	Inria
Dr. Joseph Lallemand	CNRS
Dr. Pierre Laperdrix	CNRS
Dr. Vincent Laporte	Inria
Dr. Jean-Marc Lasgouttes	Inria
Dr. Gaëtan Leurent	Inria
Dr. Victor Lomne	NinjaLab
Dr. Jean-Marie Madiot	Inria
Dr. Damien Marion	Université de Rennes
Dr. Stephan Merz	Inria
Dr. Raphaël Monat	Inria
Honorary Prof. Traian Muntean	Aix-Marseille University
Dr. Valérie Ménessier-Morain	Sorbonne Université
Dr. Renzo E. Navas	IMT Atlantique
Dr. Fabrice Neyret	CNRS
Dr. Andrea Oliveri	EURECOM
Dr. Cristina Onete	Université de Limoges
Dr. Michele Orrù	CNRS
Prof. Lafourcade Pascal	University Clermont Auvergne
Dr. Gwendal Patat	Université de Rennes
Dr. Léo Perrin	Inria

Dr. Virgile Prevosto	Université Paris-Saclay
Dr. Rémi Prébet	Inria, ENS Lyon
Dr. Maxime Puys	Université Clermont Auvergne
Dr. Maïwenn Racouchot	Université Paris-Saclay
Dr. Clara Rigaud	Ecole Centrale Lyon
Dr. Yann Rotella	University Paris-Saclay, University of Versailles Saint-Quentin en Yvelines
Dr. Merve Sahin	Personal capacity
Dr. Guillaume Scerri	ENS Paris Saclay
Dr. Bruno Scherrer	Inria
Dr. Alan Schmitt	Inria
Dr. André Schrottenloher	Inria
Dr. Sylvain Soliman	Inria
Emmanuel Thomé	Inria
Dr. Gael Varoquaux	Inria
Dr. Malisa Vucinic	Inria
Rigo Wenning	GEIE ERCIM
Prof. Melek Önen	EURECOM

Greece

Prof. Stefanos Gritzalis	University of Piraeus
Prof. Spyros Kokolakis	University of the Aegean
Dr. Ioannis Krontiris	Ubitech Ltd.
Prof. Panagiotis Rizomiliotis	Harokopio University of Athens
Prof. Georgios Stergiopoulos	Athens University of Economics and Business

Hungary

Dr. Boldizsar Bencsath	Budapest University of Technology and Economics
Dr. Gergely Biczók	Budapest University of Technology and Economics
Prof. Levente Buttyan	Budapest University of Technology and Economics
Dr. Papp Dorottya	Budapest University of Technology and Economics
Dr. Andras Gazdag	Budapest University of Technology and Economics
Dr. Tamás Holczer	BME

Iceland

Dr. Hans P. Reiser, Prof.	Reykjavik University
Prof. Giovanni Apruzzese	University of Reykjavik

Ireland

Dr. Abeba Birhane	Trinity College Dublin
Dr. Ciara Bracken-Roche	Maynooth University
Prof. John G. Breslin	University of Galway
Dr. Róisín Á Costello	Trinity College Dublin
Dr. Stephen Farrell	Trinity College Dublin
Dr. Elizabeth Farries	University College Dublin
Dr. Rónán Kennedy	University of Galway
Prof. Douglas Leith	Trinity College Dublin
Prof. David Malone	Maynooth University
Dr. TJ McIntyre	University College Dublin, Digital Rights Ireland
Dr. Maria Helen Murphy	Maynooth University

Prof. Eoin O'Dell	Trinity College Dublin
Dr. Harshvardhan Pandit	Trinity College Dublin
Dr. Maria Grazia Porcedda	Trinity College Dublin
Dr. Kris Shrishak	ICCL - Enforce

Israel

Dr. Oshrat Ayalon	University of Haifa
Prof. Orr Dunkelman	University of Haifa
Dr. Eyal Ronen	Tel Aviv University
Dr. Mahmood Sharif	Tel Aviv University

Italy

Prof. Giovanni Agosta	Politecnico di Milano
Prof. Antonino Ali	University of Trento
Prof. Marco Baldi	Università Politecnica delle Marche
Prof. Alessandro Barenghi	Politecnico di Milano
Dr. Andrea Bontempelli	University of Trento
Maria Claudia Buzzi	National Research Council (CNR)
Prof. Stefano Calzavara	Università Ca' Foscari Venezia
Dr. Davide Carnemolla	University of Catania
Prof. Bruno Crispo	University of Trento
Dr. Daniele Cono D'Elia	Sapienza University of Rome
Dr. Franco Dinelli	National Research Council (CNR)
Dr. Michele Ferrazzano	University of Modena and Reggio Emilia
Dr. Daniele Friolo	Sapienza University of Rome

Dr. Marco Giraudo	University of Turin
Dr. Marco Grassia	University of Catania
Prof. Riccardo Lazzeretti	Sapienza University of Rome
Prof. Juan Carlos De Martin	Politecnico de Torino
Francesco Migliaro	University of Catania
Prof. Emmanuela Orsini	Bocconi University
Prof. Gerardo Pelosi	Politecnico di Milano
Dr. Simone Perriello	Politecnico di Milano
Prof. Giuseppe Persiano	University of Salerno
Prof. Maria Chiara Pievatolo	University of Pisa
Dr. Maura Pintor	University of Cagliari
Prof. Leonardo Querzoni	Sapienza University of Rome
Prof. Alessandra De Rossi	University of Torino
Dr. Paolo Santini	Università Politecnica delle Marche
Dr. Edoardo Signorini	Personal capacity
Prof. Andrea Trentini	Università degli Studi di Milano
Dr. Carmela Trimarchi	National Research Council (CNR)
Prof. Daniele Venturi	Sapienza University of Rome
Prof. Stefano Zanero	Politecnico di Milano

Lebanon

Prof. Dr. Nadim Kobeissi	American University of Beirut
--------------------------	-------------------------------

Luxembourg

Dr. Afonso Arriaga	University of Luxembourg
--------------------	--------------------------

Prof. Gabriele Lenzini	University of Luxembourg
Prof. Dr. Sjouke Mauw	University of Luxembourg
Dr. Peter Roenne	University of Luxembourg
Prof. Dr. Peter Y A Ryan	University of Luxembourg
Dr. Felix Stutz	University of Luxembourg
Dr. Aleksei Udovenko	University of Luxembourg

New Zealand

Hon. Prof. Brian E. Carpenter	Prof. Brian E. Carpenter
-------------------------------	--------------------------

Norway

Dr. Tor E. Bjorstad	mnemonic AS
Dr. Carlos Cid	Simula UiB
Prof. Kristian Gjøsteen	Norwegian University of Science and Technology
Prof. Danilo Gligoroski	Norwegian University of Science and Technology
Dr. Hans Heum	Norwegian University of Science and Technology
Dr. Erik Hjelmås	Norwegian University of Science and Technology
Prof. Katrien De Moor	Norwegian University of Science and Technology
Prof. Tjerand Silde	Norwegian University of Science and Technology
Dr. Martijn Stam	Simula UiB
Prof. Michael Kirkedal Thomsen	University of Oslo
Dr. Mohsen Toorani	University of South-Eastern Norway
Prof. Staal A. Vinterbo	Norwegian University of Science and Technology
Prof. Øyvind Ytrehus	University of Bergen

Dr. Morten Øygarden

Simula UiB

Philippines

Prof. Rom Feria

University of the Philippines

Poland

Prof. Stefan Dziembowski

University of Warsaw

Portugal

Prof. Ana Aguiar

University of Porto

Prof. Paulo Azevedo

Universidade do Minho

Prof. Luis Soares Barbosa

Universidade do Minho

Prof. Manuel Barbosa

University of Porto

Prof. Manuel Eduardo
Carvalho Duarte Correia

University of Porto

Prof. Kevin Gallagher

NOVA School of Science and Technology

Prof. Francisco Almeida Maia

University of Porto

Prof. Rolando Martins

University of Porto

Prof. Nelma Moreira

University of Porto

Dr. Hugo Pacheco

Universidade do Minho

Prof. Nuno Pereira

Polytechnic Institute of Porto

Prof. Rui Prior

University of Porto

Prof. José Proença

University of Porto

Prof. Nuno Santos

INESC-ID, University of Lisbon

Prof. João Vilela

University of Porto

Slovenia

Prof. Marko Hölbl	University of Maribor
Dr. Boštjan Kežmah	University of Maribor
Dr. Tomislav Rozman	BICERO Ltd.

South Korea

Prof. Sang Kil Cha	KAIST
--------------------	-------

Spain

Prof. Isaac Agudo	University of Malaga
Dr. David Arroyo	CSIC
Dr. Marta Bellés-Munoz	Personal capacity
Prof. Pino Caballero-Gil	Universidad de La Laguna
Dr. Ignacio Cascudo	IMDEA Software Institute
Prof. Jordi Castella-Roca	Universitat Rovira i Virgili
Prof. Josep Domingo-Ferrer	Universitat Rovira i Virgili
Dr. Luis Bernal Escobedo	University of Murcia
Dr. Dario Fiore	IMDEA Software Institute
Prof. Jose Maria de Fuentes	University Carlos III of Madrid
Dr. Marco Guarnieri	IMDEA Software Institute
Prof. Jordi Herrera-Joancomarti	Universitat Autònoma de Barcelona
Prof. Javier Lopez	University of Malaga
Prof. Lorena González Manzano	University Carlos III of Madrid

Prof. Yod Samuel Martin-Garcia	Universidad Politecnica de Madrid
Dr. Pedro Moreno-Sanchez	IMDEA Software Institute
Dr. Antonio Nappa	Zimperium Inc.
Prof. Jose A. Onieva	University of Malaga
Dr. Cristina Perez-Sola	Universitat Autònoma de Barcelona
Dr. Georgios Portokalidis	IMDEA Software Institute
Prof. Ruben Rios	University of Malaga
Dr. Jesus Garcia Rodriguez	University of Murcia
Prof. Dr. Ricardo J. Rodríguez	University of Zaragoza
Prof. Rodrigo Roman	University of Malaga
Dr. Enrique Soriano-Salvador	Universidad Rey Juan Carlos
Prof. Juan Tapiador	University Carlos III of Madrid
Prof. Maria Isabel Gonzalez Vasco	University Carlos III of Madrid
Dr. Niki Vazou	IMDEA Software Institute

Sweden

Dr. Simon Bouget	RISE Research Institutes of Sweden
Dr. Fredrik Dahlgren	Trail of Bits
Dr. Christoph Egger	Chalmers University of Technology
Dr. Lars-Henrik Eriksson	Uppsala University
Prof. Simone Fischer-Hübner	Karlstad University, Chalmers University of Technology
Alfonso Iacovazzi	RISE Research Institutes of Sweden
Prof. Dr.-Ing. Meiko Jensen	Karlstad University
Dr. Adrian Perez Keilty	Chalmers University

Dr. Agnieszka Kitkowska	Jönköping University
Dr. Victor Morel	Chalmers University of Technology
Elena Pagnin	Chalmers University of Technology and University of Gothenburg
Dr. Justin Pearson	Uppsala University
Dr. Tobias Pulls	Karlstad University
Dr. Apostolos Pyrgelis	RISE Research Institutes of Sweden
Dr. Filip Strömbäck	Linköping University
Dr. Iraklis Symeonidis	Personal capacity
Dr. Marco Tiloca	RISE Research Institutes of Sweden
Prof. Bjorn Victor	Uppsala University

Switzerland

Prof. David Basin	ETH Zurich
Dr. Andrea Basso	IBM Research
Dr. Ward Beullens	IBM Research
Dr. Cecilia Boschini	ETH Zurich
Dr. Jeffrey Burdges	Web 3 foundation
Prof. Dr. Srdjan Capkun	ETH Zurich
Antonis Chariton	Cisco
Dr. Anastasija Collen	University of Geneva
Dr. Ana-Maria Cretu	EPFL
Dr. Elizabeth Crites	Web3 Foundation
Dr. Tommaso Gagliardini	Horizen Labs
Prof. Jean-Pierre Hubaux	EPFL

Frederic Jacobs	Personal capacity
Dr. Pascal Junod	Personal capacity
Dr. Kari Kostinen	ETH Zurich
Dr. Anil Kurmus	IBM Research
Dr. Lenka Marekova	ETH Zurich
Prof. Simon Mayer	University of St. Gallen
Dr. Simon-Philipp Merz	ETH Zurich
Prof. Kenneth Paterson	ETH Zurich
Prof. Mathias Payer	EPFL
Prof. Adrian Perrig	ETH Zurich
Prof. Kaveh Razavi	ETH Zurich
Dr. Raphael M. Reischuk	National Test Institute for Cybersecurity NTC
Dr. Benjamin Rothenberger	Zühlke
Dr. Ralf Sasse	ETH Zurich
Dr. Theresa Stadler	EPFL
Dr. Bjoern Tackmann	DFINITY Stiftung
Dr. Piet De Vaere	ETH Zurich
Prof. Isabel Wagner	University of Basel

Taiwan

Dr. Matthias Kannwischer	Chelpis Quantum Corp
--------------------------	----------------------

The Netherlands

Dr. Abhishta Abhishta	University of Twente
Dr. Gunes Acar	Radboud University

Prof. Luca Allodi	Eindhoven University of Technology
Dr. Greg Alpar	Radboud University
Dr. Jacob Appelbaum	Eindhoven University of Technology
Dr. Jaya Baloo	Aisle
Prof. Lejla Batina	Radboud University
Prof.Dr. Bibi van den Berg	Leiden University
Prof. Jeanne Mifsud Bonnici	University of Groningen
Prof. Dr. Frederik Zuiderveen Borgesius	Radboud University
Prof. Dr. Herbert Bos	VU Amsterdam
Dr. Ir. Jurjen N.E. Bos	Worldline
Dr. Ir. Xavier de Carné de Carnavalet	Radboud University
Prof. Andrea Continella	University of Twente
Dr. Lorenzo Dalla Corte	Tilburg Institute for Law, Technology and Society
Prof. Ronald Cramer	CWI, Leiden University
Prof. Joan Daemen	Radboud University
Prof. Marten van Dijk	CWI
Dr. Thijs van Ede	University of Twente
Prof.Dr. Michel van Eeten	TU Delft
Dr. Zeki Erkin	TU Delft
Dr. ir. Thomas Fabry	Maastricht University
Dr. Malvin Gattinger	University of Amsterdam
Prof. Cristiano Giuffrida	VU Amsterdam
Dr. Seda Gürses	TU Delft
Dr.-Ing. Florian Hahn	University of Twente

Prof. Dr. Cristian Hesselman	University of Twente
Prof. Dr. Jaap-Henk Hoepman	Radboud University, Karlstad University
Prof. Simone van der Hof	Leiden University
Prof. Kathrin Hövelmanns	Eindhoven University of Technology
Dr. Andreas Hülsing	Eindhoven University of Technology
Prof. Bart Jacobs	Radboud University
Dr. Slinger Jansen	Utrecht University
Dr. Konrad Kollnig	Maastricht University
Dr. ing. Ralph Koning	University of Amsterdam
Prof. Bert-Jaap Koops	Tilburg University
Dr. Matthijs Koot	University of Amsterdam
Prof. Dr. Tanja Lange	Eindhoven University of Technology
Dr. Michiel de Lange	Utrecht University
Dr. Marjolein Lanzing	University of Amsterdam, Bits of Freedom
Prof.Dr. Ronald Leenes	Tilburg University
Ad van Loon	Qiy Foundation
Prof. Eleftheria Makri	Leiden University
Dr. Luca Mariot	University of Twente
Prof. Bart Mennink	Maastricht University
Prof. Dr. Lokke Moerel	Tilburg University
Dr. Giovane Moura	TU Delft
Prof. Dr. ir. Lambert J.M. Nieuwenhuis	University of Twente
Dr. Sabine Oechsner	VU Amsterdam
Dr. Kostas Papagiannopoulos	University of Amsterdam

Dr. Subhasree Patro	Eindhoven University of Technology
Dr. Paola de Perthuis	CWI
Dr. Ir. Joop van de Pol	Trail of Bits
Dr.ir. Erik Poll	Radboud University
Dr. Cristina Del Real	Leiden University
Dr. Nicolas Resch	University of Amsterdam
Prof. Dr. ir. Roland van Rijswijk-Deij	University of Twente
Dr. Ashish Sai	Maastricht University
Prof. Simona Samardjiska	Radboud University
Prof. Christian Schaffner	University of Amsterdam
Dr. Theodor Schnitzler	Maastricht University
Dr. Hanna Schraffenberger	Radboud University
Dr. Ir. Roland Siemons	Clean Fuels B.V.
Dr. Tommy van Steen	Leiden University
Dr. Samaneh Tajalizadehkhoob	ICANN
Prof. Monika Trimoska	Eindhoven University of Technology
Dr. Christine Utz	Radboud University
Dr. Heloise Vieira	Eindhoven University of Technology
Dr. Jeroen van der Ham-de Vos	University of Twente
Dr. Thom Wiggers	Personal capacity
Jeroen Willemsen	OWASP
Dr. Mengyuan Zhang	VU Amsterdam
Dr. Yury Zhauniarovich	TU Delft

Turkey

Prof. Cihangir Tezcan Middle East Technical University

United Arab Emirates

Prof. Mihalis Maniatakos New York University Abu Dhabi

Prof. Christina Poepper New York University Abu Dhabi

Prof. Sandra Siby New York University Abu Dhabi

United Kingdom

Prof. Martin Albrecht King's College London

Dr. Panagiotis Andriotis University of Birmingham

Dr. Martin Atkins Mission Critical Applications Limited

Prof. Eerke Boiten De Montfort University

Prof. Ioana Boureanu University of Surrey

Dr. Xavier Carpent University of Nottingham

Dr. Giovanni Cherubin Microsoft Research

Prof. Nathan Clarke University of Plymouth

Dr. Simone Colombo King's College London

Dr. François Dupressoir University of Bristol

Prof. Tariq Elahi University of Edinburgh

Prof. Elaine Fahey City St. Georges, University of London

Dr. Joël Felderhoff King's College London

Honorary Prof. Jens Groth Nexus, University College London

Dr. Neil Hanley Queens University Belfast

Dr. Weijia He	University of Southampton
Prof. Alice Hutchings	University of Cambridge
Dr. Dennis Jackson	Mozilla
Dr. Aaron S. Jackson	University of Dundee
Prof. Rikke Bjerg Jensen	Royal Holloway, University of London
Prof. Vasilis Katos	Bournemouth University
Prof. Markulf Kohlweiss	University of Edinburgh
Dr. Kaspar Rosager Ludvigsen	Durham University
Prof. Keith Martin	Royal Holloway, University of London
Prof. Andrew Martin	University of Oxford
Prof. Sarah Meiklejohn	University College London
Dr. Kevin Milner	Quantinuum
Prof. Andy Phippen	Bournemouth University
Dr. Eamonn Postlethwaite	King's College London
Prof. Awais Rashid	University of Bristol
Prof. Kasper Rasmussen	University of Oxford
Prof. Steve Schneider	University of Surrey
Dr. Alessandro Di Stefano	Red Hat
Dr. Fernando Virdia	University of Surrey
Dr. Christian Weinert	Royal Holloway, University of London
Prof. Alan Woodward	University of Surrey

United States of America

Prof. Jonathan Aldrich	Carnegie Mellon University
Prof. Lujo Bauer	Carnegie Mellon University

Prof. Antonio Bianchi	Purdue University
Prof. L Jean Camp	Indiana University
Prof. Nicolas Christin	Carnegie Mellon University
Dr. Daniel Collins	New York University, Hebrew University
Prof. Lorrie Cranor	Carnegie Mellon University
Dr. Felix Engelmann	Ohio State University
Prof. Christina Garman	Purdue University
Prof. Matthew D. Green	Johns Hopkins University
Prof. Paul Grubbs	University of Michigan
Dr. Joseph Lorenzo Hall	Internet Society
Prof. Vasileios Kemerlis	Brown University
Prof. Susan Landau	Tufts University
Prof. Anna Lysyanskaya	Brown University
Prof. Michelle Mazurek	University of Maryland
Prof. Riccardo Paccagnella	Carnegie Mellon University
Prof. Michalis Polychronakis	Stony Brook University
Dr. Niels Provos	Security Blueprints, LLC
Prof. Amir Rahmati	Stony Brook University
Prof. Aanjhan Ranganathan	Northeastern University / ETH Zürich
Prof. Nitesh Saxena	Texas A&M University
Prof. Sarah Scheffler	Carnegie Mellon University
Prof. Adam Shostack	Personal Capacity
Dr. Daniel Smullen	Personal capacity
Prof. Jonathan Takeshita	Old Dominion University
Dr. Pingbo Tang	Carnegie Mellon University

Dr. Alin Tomescu

Aptos Labs

Prof. Blase Ur

University of Chicago

Prof. Riad Wahby

Carnegie Mellon University

Prof. Chau-Wai Wong

North Carolina State University

Prof. Daniel Zappala

Brigham Young University