



Bundesministerium  
des Innern, für Bau  
und Heimat



# Gesamtgesellschaftliche Erklärung zur Cybersicherheit



**Quadrigavertreter für die Zivilgesellschaft**

**Herr Klaus Müller**

Vorstand Verbraucherzentrale Bundesverband e.V.



**Quadrigavertreterin für die Wissenschaft**

**Frau Prof. Dr. Mira Mezini**

Professorin für Informatik an der TU Darmstadt



**Quadrigavertreterin für die Wirtschaft**

**Frau Claudia Nemat**

Mitglied des Vorstands der Deutschen Telekom



**Quadrigavertreter für den Staat**

**Herr Prof. Dr. Günter Krings**

Parlamentarischer Staatssekretär beim Bundesminister  
des Innern, für Bau und Heimat

# Cybersicherheit als gesamtgesellschaftliche Herausforderung

---

Die IT- und Datensicherheit ist für den Prozess des digitalen Wandels von herausragender und zentraler Bedeutung. Unternehmen und öffentliche Einrichtungen digitalisieren zunehmend ihre Prozesse, Aufgaben- und Geschäftsfelder. Haushalte, Verbraucherinnen und Verbraucher setzen zunehmend auf vernetzte und smarte Produkte, die Wissenschaft lehrt und forscht zu den Grundlagen und Konzepten der Cybersicherheit und ihrer Anwendung. Die Digitalisierung hat eine Schlüsselrolle für Fortschritt, Wettbewerbsfähigkeit, Wohlstand und Nutzen in der modernen Gesellschaft. Die wachsende Sensibilisierung für Themen der Cybersicherheit in allen Gesellschaftsbereichen spielt eine maßgebliche Rolle für eine sichere und geschützte Interaktion zwischen den verschiedenen gesellschaftlichen Akteuren in Deutschland.

Digitalisierung kann nur dann erfolgreich und nachhaltig gelingen, wenn Fragen der Cybersicherheit hinreichend berücksichtigt werden. Dies umfasst sowohl die Entwicklung von sicheren Technologien, Produkten und Dienstleistungen durch die Hersteller als auch die Bildung und Ausbildung der Anwender, angefangen bei Kindern und Jugendlichen über das Studium bis hin zur berufsbegleitenden Weiterbildung. Die konsequente Berücksichtigung von Cybersicherheit reduziert die Verwundbarkeit von Anwendern aller Gesellschaftsgruppen und bietet einen Wettbewerbsvorteil auf Herstellerseite. Cybersicherheit ist Querschnitts- und Schlüsseltechnologie für die Digitalisierung und mit der Weiterentwicklung von Technologien und Angriffsszenarien steht sie immer wieder vor neuen Herausforderungen.

Sicheres und selbstbestimmtes Handeln in einer digitalisierten Welt erfordert einen Ansatz, der alle gesellschaftlichen Gruppen spezifisch einbindet: Zivilgesellschaft, Wissenschaft, Wirtschaft und Staat. Mit dem Nationalen Pakt Cybersicherheit wurde eine Initiative ins Leben gerufen, welche sich diesem Ansatz widmet, um hierdurch bestehende Initiativen und Akteure im Bereich der Cybersicherheit zu identifizieren, die vertrauensvolle Zusammenarbeit in der Gesamtgesellschaft auszubauen und die zielgruppenspezifische Sensibilisierung vor Gefahren des Cyberraums zu intensivieren.

Nachdem im ersten Schritt mit dem Online-Kompendium Cybersicherheit ein bislang einzigartiger, strukturierter Überblick über die deutsche Cybersicherheitslandschaft erstellt und veröffentlicht wurde,

gilt es nun mit dieser Erklärung die gemeinsame Verantwortung für digitale Sicherheit in einem nationalen Pakt festzuschreiben und gleichzeitig die Umsetzungsphase des Paktes einzuleiten.

Der Nationale Pakt Cybersicherheit bietet eine Chance, die Rahmenbedingungen der Cybersicherheit zum Nutzen aller Gesellschaftsgruppen weiter zu entwickeln und stellt einen nationalen Beitrag zum "Paris Call for Trust & Security in Cyberspace" des französischen Präsidenten Emmanuel Macron dar.

Wir, die Quadriga, bestehend aus Herrn Klaus Müller, Frau Prof. Dr. Mira Mezini, Frau Claudia Nemat und Herrn Prof. Dr. Günter Krings, vertreten die Gesellschaftsgruppen Zivilgesellschaft, Wissenschaft, Wirtschaft und Staat und wollen in dieser gesamtgesellschaftlichen Erklärung unsere vertrauensvolle Zusammenarbeit zur Stärkung der Cybersicherheit in Deutschland bekräftigen.

*1. „Wir betonen, dass sich die Cybersicherheit in der Zivilgesellschaft vor allem durch ihre Heterogenität an Interessenlagen, Themenschwerpunkten und Organisationsformen kennzeichnet. Diese Vielfalt an Betrachtungswinkeln, Entwicklungsansätzen und fachlichen Herausforderungen gilt es zu nutzen und zu fördern. So können einzigartige Projekte entstehen, die die deutsche Cybersicherheitslandschaft und ihre Akteure stärken.“*

*2. „Wir bekräftigen, dass Privatanwender unterstützt werden, sichere digitale Produkte zu erkennen und auf Mindeststandards dieser Produkte vertrauen zu können. Diese Rahmenbedingungen gilt es gemeinsam zu schaffen, international zu harmonisieren und stetig weiterzuentwickeln.“*

*3. „Wir betonen, dass die Grundlage für adaptive und risikobasierte Normen und Standards gemeinsam geschaffen werden sollte, damit den unterschiedlichen Anforderungen diverser Akteure und Gesellschaftsgruppen bei der Regulierung Genüge getan werden kann.“*

*4. „Wir erkennen, dass Zertifizierungen bei der Erhöhung des Cybersicherheitsniveaus eine wichtige Rolle spielen und dass die Einführung und Erlangung entsprechender Zertifikate unterstützt werden sollte, wo dies nicht oder nur unzureichend aus eigener Kraft geschehen kann.“*

5. „Wir begrüßen die erfolgreiche Positionierung der Cybersicherheitsforschung Deutschlands auf internationalem Spitzenniveau. Um dieses Niveau aufrecht erhalten zu können, muss sich die Forschung im internationalen Wettbewerb weiterentwickeln. Dafür ist es immanent wichtig, sowohl die Grundlagenforschung als auch die anwendungsorientierte Forschung an der potenziellen Wirkmacht ihrer Beiträge für die verschiedenen Gesellschaftsgruppen zu orientieren. Dies umfasst das Aufgreifen und die Verwertung von Ergebnissen und Erkenntnissen durch Zivilgesellschaft, Wirtschaft und Staat sowie durch die Wissenschaft selbst. Aus Forschung und Entwicklung wird Spitzenforschung, wenn ihre Ergebnisse entscheidende Beiträge liefern, um die Welt von morgen besser zu machen. Dies umfasst insbesondere den Transfer von Ergebnissen in die praktische Anwendung.“

6. „Wir bekräftigen, dass die Cybersicherheitsforschung aufgrund ihrer großen Bedeutung in hinreichendem Umfang gefördert werden muss. Die inhaltliche Ausrichtung der Forschungsarbeiten sollte sich eng an dem Nutzen aller Gesellschaftsgruppen orientieren und so angelegt sein, dass möglichst viele davon profitieren können. Hierfür braucht es den dauerhaften Dialog zwischen der Wissenschaft und den anderen Gesellschaftsgruppen.“

7. „Wir betonen, dass die Wissenschaft förderliche Rahmenbedingungen benötigt, mit denen man die besten Köpfe weltweit gewinnen sowie halten kann und welche zur Entwicklung der herausragenden Wissenschaftlerinnen und Wissenschaftler von morgen beiträgt. Schnelle Reaktionsfähigkeit in der Wissenschaft braucht Entscheidungsprozesse, die möglichst unbürokratisch ausgelegt sind.“

8. „Wir erkennen, dass die Ausbildung von spezialisierten Fachkräften weiterentwickelt und ausgeweitet wird, um den hohen Bedarf an Spezialistinnen und Spezialisten in den verschiedensten Branchen und von Organisationen unterschiedlichster Größen zu decken. Hierzu sollten die Aus- und Weiterbildung verbreitert, Fachausprägungen geschaffen und alternative Karrierewege gefördert werden.“

9. „Wir regen an, dass pragmatische Hilfestellungen zum Verstehen von und zum sicheren Umgang mit IT zu einem anerkannten und integralen Bestandteil der (vor-)schulischen und beruflichen Ausbildung werden, um das persönliche Sicherheitsniveau zu verbessern und den Grundstein für weiterführendes Interesse an diesem Themenbereich zu legen.“

10. „Wir bekräftigen, dass die einfache Verfügbarkeit sicherheitssteigernder Technik, wie Verschlüsselung oder automatisierte Softwaretests bzw. von offiziellen Testergebnissen, für jedermann zugänglich sein muss, um so individuelle Cybersicherheit zu fördern, aber auch Wettbewerbsfähigkeit zu erhalten. Wir wollen die Identifizierung und Verbreitung geeigneter Werkzeuge gemeinsam begleiten.“

11. „Wir bekräftigen, dass Cybersicherheit von hoher makroökonomischer Bedeutung ist und den technologischen Fortschritt maßgeblich beeinflusst, etwa im Rahmen flächendeckender Digitalisierung von Dienstleistungen oder Verwaltungsleistungen. Daher müssen Rahmenbedingungen und Inhalte gesamtgesellschaftlich erarbeitet werden.“

12. „Wir regen an, dass alle Initiativen und Akteure der Cybersicherheit den Nationalen Pakt Cybersicherheit dazu nutzen, ihre Sichtbarkeit und Transparenz zu steigern, jeweils mehr übereinander zu erfahren und dies dahingehend einzusetzen, sich mit anderen Akteuren und Initiativen übergreifend auszutauschen, zu vernetzen und gemeinsam zu wachsen. Hierfür sollten bestehende, einseitige Formate von einer zentralen Plattform abgelöst werden, auf der alle Akteure, Initiativen, Projekte und Angebote qualitätsgeprüft aufzufinden sind und miteinander interagieren können.“

13. „Wir betonen, dass eine zielgruppenspezifische Sensibilisierung vor Gefahren des Cyberraums durch eine gesamtgesellschaftliche thematische Auseinandersetzung vorangetrieben wird.“

Gemeinsam können wir viel bewegen. Wir befinden uns auf einem guten Weg zur Erreichung der erklärten Ziele und haben mit dem Nationalen Pakt Cybersicherheit die organisatorischen Weichen für ein sicheres Miteinander in der digitalen Welt gestellt.

**Klaus Müller**, Verbraucherzentrale Bundesverband

**Prof. Dr. Mira Mezini**, TU Darmstadt

**Claudia Nemat**, Deutsche Telekom

**Prof. Dr. Günter Krings**, Bundesministerium des Innern, für Bau und Heimat

**Werden Sie Teil des Nationalen Pakts!**

Unterstützen Sie den Nationalen Pakt Cybersicherheit bei der Umsetzung der vorgeschlagenen Maßnahmen und treten Sie der gesamtgesellschaftlichen Erklärung bei. Dies kann entweder in allgemeiner Form erfolgen,

beispielsweise durch eine namentliche Nennung auf der Internetseite des Pakts. Eine andere Möglichkeit wäre die konkrete Unterstützung einer der o.g. Maßnahmen durch die Initiierung und Umsetzung konkreter Projekte oder Maßnahmen, die Sie durch Ihre Institution bzw. Unternehmen umsetzen.