



GESELLSCHAFT
FÜR INFORMATIK

Berlin, 28. Juni 2023

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

zur Nationalen Sicherheitsstrategie der
Bundesregierung vom 14. Juni 2023



Am 14. Juni 2023 hat die Bundesregierung [die Nationale Sicherheitsstrategie „Wehrhaft. Resilient. Nachhaltig“](#) vorgestellt, mit der sie umfassend sicherheitspolitische Herausforderungen zusammenfasst und beschreibt, wie sie diesen begegnen will. Die Strategie verfolgt das politische Konzept der „Integrierten Sicherheit“. Darunter versteht die Bundesregierung ein „Zusammenwirken aller relevanten Akteure, Mittel und Instrumente“ für die nationale Sicherheit. Wesentliche Teile der Nationalen Sicherheitsstrategie widmen sich dem Thema Cybersicherheit, zu denen die Gesellschaft für Informatik (GI) im Folgenden Stellung bezieht.

1. Cybersicherheit als wichtiger Teil der Sicherheitsstrategie

Die GI begrüßt die Veröffentlichung einer Nationalen Sicherheitsstrategie, mit der die Bundesregierung das Thema Sicherheit als ressort- und grenzübergreifende Herausforderung adressiert. Cybersicherheit ist angesichts der weiter voranschreitenden Digitalisierung aller Lebensbereiche eine besonders relevante sicherheitspolitische Herausforderung. Es ist daher richtig und wichtig, dass diese in der Nationalen Sicherheitsstrategie prominent behandelt wird. Die Strategie spricht viele wichtige Aspekte der Cybersicherheit an. Dazu zählt die GI einen verbesserten behördlichen Austausch, grenzübergreifende Zusammenarbeit sowie die Herstellung gesamtstaatlicher Resilienz, insbesondere für den Bereich Kritischer Infrastrukturen.

2. Prävention statt intrusiver Maßnahmen

Die GI unterstützt den Plan der Bundesregierung, Kompetenzen zur Cyberabwehr auszubauen. Kritisch sieht sie, dass die Bundesregierung sich dabei nicht von offensiver Cyberabwehr distanziert, mit der die Infrastruktur eines Angreifenden repressiv geschädigt werden soll (sog. intrusive Maßnahmen). Die Formulierung, dass Hackbacks „prinzipiell“ abgelehnt werden, lässt (wie schon im Koalitionsvertrag) Raum für Interpretationen und nicht akzeptable Ausnahmen (vgl. [GI Policy Brief „Aktive Cyberabwehr im Angesicht einer sicherheitspolitischen Neuaufstellung“](#)).

3. Ein sicheres Internet durch Responsible Disclosure

Die GI begrüßt ausdrücklich, dass sich die Bundesregierung zu einem freien Internet bekennt und für ein Recht auf Verschlüsselung eintreten will (S. 59). Sie weist darauf hin, dass dieses nur mit einer Offenlegung von Sicherheitslücken nach einem Responsible-Disclosure-Verfahren durchgesetzt werden kann. Mit geheim gehaltenen Sicherheitslücken kann auch Verschlüsselungssoftware umgangen werden. Die Geheimhaltung von Sicherheitslücken gefährdet zudem viele weitere von der Sicherheitslücke betroffene Akteure und kann zu massiven gesellschaftlichen und wirtschaftlichen Schäden führen. Vorgaben zur Responsible Disclosure für alle Bundesbehörden sieht die GI daher als wirksamen Schutz vor Bedrohungen aus dem Cyberraum.

4. Technologische Souveränität durch Open Source stärken

Die GI bedauert, dass die Bundesregierung den Begriff der technologischen Souveränität nur am Rande behandelt. Technologische Souveränität, also die Fähigkeit, selbstbestimmt und unabhängig zu agieren, ist angesichts den in der Sicherheitsstrategie aufgeführten wachsenden internationalen Spannungen eine bedeutende Basis für Cybersicherheit. Um Cybersicherheit zu stärken, bedarf es freier (Open Source) Technologien, die – ganz im Sinne der in der Sicherheitsstrategie angestrebten internationalen Zusammenarbeit – von vielen, weltweit verteilten Akteuren weiterentwickelt und auf Schwachstellen geprüft wird. Die GI sieht Open Source Soft- und Hardware außerdem als wichtigen Schlüssel, um möglichst viele europäische Akteure an der Technologieentwicklung zu beteiligen und damit bislang zu langsame Entwicklungen zu beschleunigen und Sprunginnovationen zu ermöglichen.

5. Wissenschaft und Zivilgesellschaft beteiligen

Die Bundesregierung kündigt an, die Sicherheitsstrategie mit vielen weiteren Strategien konkreter auszuformulieren. Dies ist aus Sicht der GI unbedingt notwendig. Die GI begrüßt, dass die Bundesregierung zivilgesellschaftliche Organisationen bei weiteren Entwicklungen einbeziehen will (S. 58). Die Zivilgesellschaft besteht aus vielfältigen Akteuren, die die Regierung beim Thema Cybersicherheit mit innovativen Lösungen und relevanten Hinweisen bereichern können. Bei weiteren Prozessen muss sie daher ebenso wie wissenschaftliche Akteure als gleichberechtigte Stimme beteiligt werden.

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.