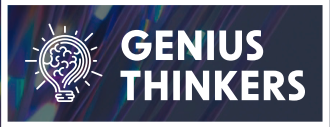


Juli '25



think about

# Digital Future

Impulse, Strategien und Lösungen  
für die Wirtschaft von morgen

## Künstliche Intelligenz

Gamechanger  
für die Wirtschaft

## Cyber Security

Schutzschild in einer  
vernetzten Welt

## Digitalisierung

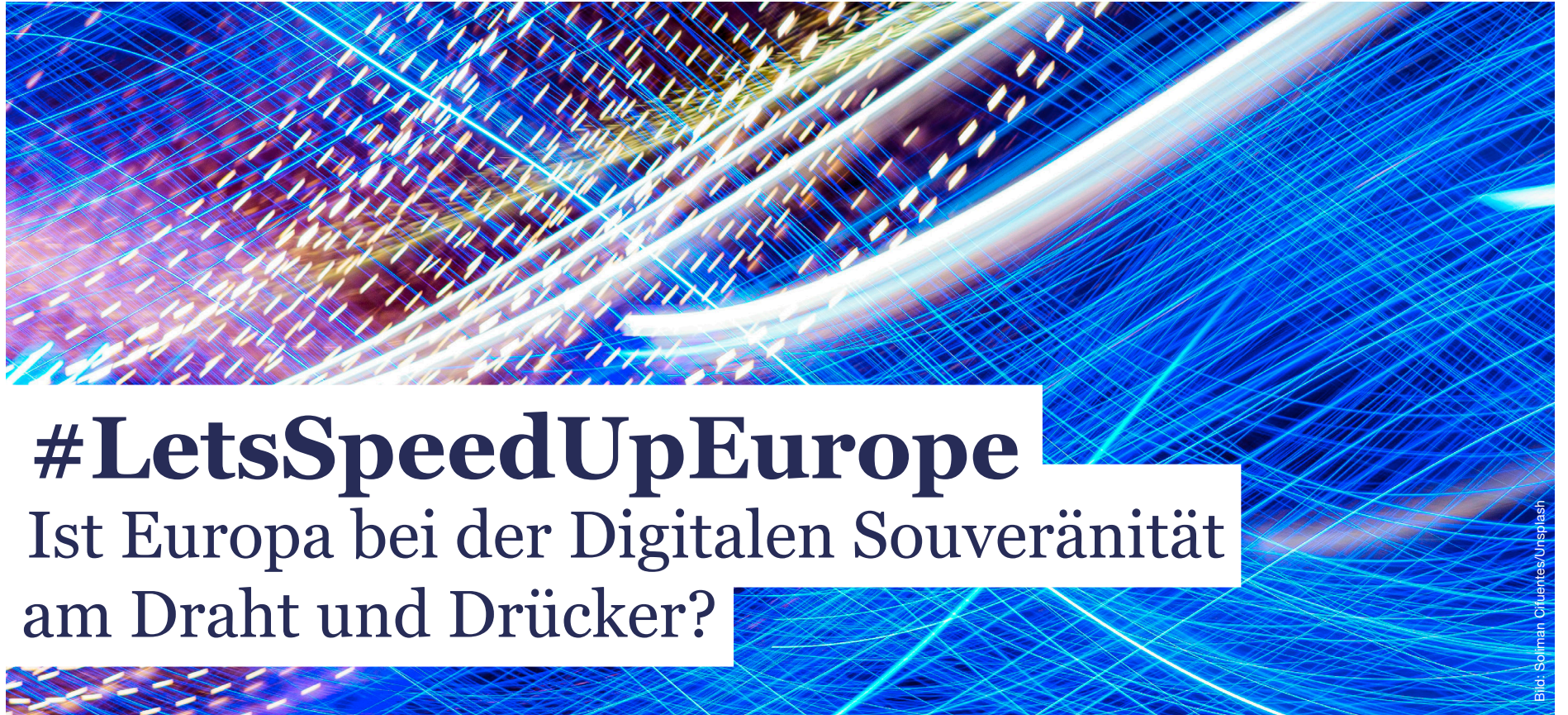
Treiber für Resilienz &  
Wachstum

## Digitale Souveränität

Europas  
Antwort

## Smart Factory

Effizienz durch  
Automatisierung



# #LetsSpeedUpEurope

## Ist Europa bei der Digitalen Souveränität am Draht und Drücker?

In seinem Buch »Digitale Souveränität für Europa« (Haufe Freiburg 2023), das viele Beiträge prominenter Politiker und Wissenschaftler vereint, setzt Herausgeber Markus Ferber auf eine dringend notwendige digitale Neuorientierung, spricht »Grundlage dafür, dass wir in Europa in Politik, Wirtschaft und Gesellschaft auch im digitalen Raum selbstbestimmt handeln und entscheiden können«.

Text Rüdiger Schmidt-Sodingen

Wo viele »etablierte Plattformen mittlerweile als De-facto-Regulierer fungieren«, so analysiert es der ehemalige Bundesregierungssprecher und Intendant des Bayerischen Rundfunks Ulrich Wilhelm, müsse Europa endlich »in die technologische Tiefe gehen und eine eigene digitale Infrastruktur entwickeln«. Das sei zwar »risikoreich und komplex, aber auch mit der enormen Chance für Europa verbunden, Abhängigkeiten zu vermeiden und auch im digitalen Raum eine positive gestaltende Rolle einnehmen zu können«.

Die eigentliche Herausforderung, so Wilhelm, liege dabei im Ausgleich ökonomischer Interessen und

gesellschaftlicher Zielvorstellungen. »Eine solche technische Infrastruktur sollte daher als Teil der öffentlichen Daseinsvorsorge begriffen werden, um der Quasi-Monopolstellung der großen Anbieter eine effektive Alternative entgegenzusetzen.« Randolph Carr und Wolfgang Ischinger, beide bis 2022 bei der Münchner Sicherheitskonferenz tätig, betonen, dass eine echte europäische Lösung nur mithilfe der USA möglich sei: »Europa muss zunächst sein digitales Haus in Ordnung bringen. Und zweitens müssen Europa und die USA das transatlantische Vertrauen im digitalen Bereich stärken.«

**Digitale Souveränität meint Kooperation, nicht Isolation**  
Prof. Dr. Utz Schliesky, Direktor des Schleswig-Holsteinischen Landtages und Vorstand des Lorenz-von-Stein-Instituts an der Kieler Christian-Albrechts-Universität gibt zu bedenken, dass digitale Räume bislang von privaten Konzernen errichtet und gesteuert werden, die auch als »Kontrolleure des Zugangs und zulässiger Aktivitäten« auftreten. Dementsprechend bestehe »zunächst einmal keine für die Souveränität erforderliche Beherrschungsmöglichkeit dieser Räume für den Staat«. Dies werfe »die Frage nach der Inhaberschaft digitaler Souveränität auf«. »In dem Begriff der digitalen Souveränität«, so Schliesky weiter, »spiegelt sich nichts Geringeres als der Kampf

des demokratischen Verfassungsstaates und der in ihm zusammengeschlossenen Bürger um die eigene politische Selbstbestimmung in digitalen Räumen und die Beherrschung dieser Räume zur Gewährleistung von Sicherheit.« Wer Volkssouveränität ernst nehme, müsse den »Ableitungs-, Zurechnungs- und Verantwortungszusammenhang zwischen Volk und Staatsgewalt in digitalen Räumen« neu konzipieren und herstellen.

Neben Plädoyers für mehr Zusammenarbeit und eine aktive Plattformregulierung kommt in dem Buch auch eine Neu- oder Reorganisation der Arbeit zur Sprache. »Die Mitarbeiter selbst sind gefordert, auf die Dynamik zu reagieren, schnell Entscheidungen zu treffen und diese selbstorganisiert umzusetzen«, so Clemens Drilling und Prof. Dr. Helmut Klausung, bevor Claudia Plattner, seit 2023 Präsidentin des Bundesamts für Sicherheit in der Informationstechnik, die unlängst eine unabhängige Cloud-Lösung mit Google einfädelt, zu mehr Optimismus aufruft. »Ja, wir liegen zurück. Aber ein Kampf geht über zwölf Runden und wir sind erst in Runde vier. Hier ist noch gar nichts entschieden. (...) Digitale Souveränität in Europa ist erreichbar. Wachsen wir über uns hinaus und schaffen wir Resultate – und das schnell. Nicht übermorgen, nicht morgen und nicht einmal heute Nachmittag. Jetzt. #LetsSpeedUpEurope!«

Genius Partner • CSE – Center of Safety Excellence GmbH

think about: Cyber Security

## Strategien für Mittelständler: Schützen Sie Ihre Anlagen vor Cybergefahren!

Cybergefahren werden vom Mittelstand oft unterschätzt. Cyberangriffe auf mittelständische Anlagen nehmen zu. In einem Experteninterview spricht Professor Dr. Jürgen Schmidt, Executive Director des CSE Center of Safety Excellence gGmbH in Pfnitztal, über den Schutz vor Cyberangriffen auf mittelständische Unternehmen.

Herr Schmidt, Sie leiten das CSE Center of Safety Excellence, haben über 25 Jahre bei BASF gearbeitet und lehren an den Universitäten in Karlsruhe und Kaiserslautern. Seit Jahren setzen Sie sich für den Schutz von Anlagen vor Cyberangriffen ein, nun auch für kleine und mittlere Unternehmen (KMU). Sind KMU in Deutschland tatsächlich von Hackern bedroht? Ja, insbesondere bei KMUs mit Produktionsanlagen sind die Angriffe intensiver geworden. Im Mai haben Hacker zwei

Professor Dr. Jürgen Schmidt,  
Executive Director, CSE Center  
of Safety Excellence gGmbH



Biogasanlagen in Norddeutschland angegriffen und erhebliche Schäden verursacht. Viele Betreiber können sich kaum vorstellen, dass sie Ziel solcher Angriffe sind.

**Wie unterstützt das CSE Center of Safety Excellence diese Unternehmen?**

Das CSE entwickelt die Software EvaSecur, die ab 2026 kostenfrei angeboten und vom Bundesministerium für Wirtschaft und Energie gefördert wird. EvaSecur deckt die regulatorischen Vorgaben bedarfsgerecht ab und erhöht das Sicherheitsniveau, die Produktivität der Anlagen sowie das Wissen im Bereich Cybersecurity. Dies gilt für Anlagen wie Biogas, Kraftwerke, Windenergie, Verpackung und Produktion, die von Zehntausenden Unternehmen in Deutschland betrieben werden. Details siehe [www.evasecur.de](http://www.evasecur.de).

**Kann EvaSecur ohne IT-Fachkenntnisse angewendet werden?**

Ja! EvaSecur bietet eine unkomplizierte 80%-Lösung – den Basis-Schutz. Die

Anwender sollen die Hemmschwelle überwinden, im fachfremden Bereich Cybersecurity aktiv zu werden.

**Berücksichtigt EvaSecur auch die gesetzlichen Anforderungen?**

Ja, EvaSecur wird aus fünf Modulen bestehen, die sich an den gesetzlichen Vorgaben und den Empfehlungen des Basis-Grundschutzes orientieren: (1) Gefahrenbeurteilung einer Anlage, (2) Asset-Liste mit den relevanten Assets des Produktionsnetzwerks, (3) Schwachstellenanalyse, (4) Liste mit Gegenmaßnahmen und (5) Awareness-Training zum Thema Cybersecurity. Mit EvaSecur wird die Beurteilung von Maßnahmen abhängig von den Risiken in einer Anlage durchgeführt. CSE entwickelt EvaSecur in enger Zusammenarbeit mit Betreibern.

