



12. SynergyLab der GWS e.V.

Das SynergyLab ist der Begegnungsraum für Mitglieder und Gäste der *Gesellschaft für Wirtschafts- und Sozialkybernetik (GWS) e.V.*, um gemeinsam aktuelle Herausforderungen in Organisationen und Gesellschaft systemisch zu analysieren und zu diskutieren. Hier treffen Wissenschaft, Praxis und innovative Ideen aufeinander – in einem offenen Format, das zum Mitdenken und Mitgestalten einlädt.

Regelmäßig bieten wir Impulsvorträge zu spannenden Themen rund um intelligente Organisationen, Systemdenken, kollektive Intelligenz und kybernetische Ansätze. Nach einem kurzen Input folgt eine offene moderierte Diskussion, in der die Teilnehmer ihre Erfahrungen, Erkenntnisse und Fragen einbringen können.

Impulsvortrag **Prof. Dr. Laura Georg Schaffner: „Cybersecurity als komplexer Problemraum: Verborgene Dynamiken und kollektive Entscheidungsfähigkeit“**

Format Impulsvortrag und offene Diskussion
25 Teilnehmende aus dem Kreis der GWS und Gäste aus Wissenschaft und Praxis

Datum 30. September 2026

Referentin **Prof. Dr. Laura Georg Schaffner** ist Associate Professor an der EM Strasbourg Business School der Universität Straßburg. Ihre Arbeit verbindet Forschung zu Strategie, Governance und Cybersicherheit mit langjähriger Führungserfahrung in der Wirtschaft. Unter anderem war sie bei AXA als Group Head of Security Strategy & Awareness tätig und leitete zuvor das NISLab, eines der größten europäischen Forschungslabore für Cybersicherheit. Darüber hinaus ist sie als Expertin für die Research Executive Agency (REA) der Europäischen Kommission tätig und Non-Resident Fellow am Center for Long-Term Cybersecurity der University of California, Berkeley.



Management Summary

Kontext & Ziel

Im 12. SynergyLab stellte Laura Georg Schaffner Ergebnisse eines mehrjährigen Forschungsprojekts zur Cybersecurity-Governance in Aufsichts- und Verwaltungsräten vor. Ausgangspunkt ist die Beobachtung, dass Probleme auf Board-Ebene nicht allein durch fehlende Informationen oder technische Expertise entstehen. Entscheidend ist vielmehr, welche Aspekte eines komplexen Problemraums überhaupt sichtbar werden, wie Boardmitglieder diese interpretieren und welche Rückkopplungen, Verzögerungen und indirekten Wirkungen dadurch in der Governance entstehen.

Der Vortrag verband qualitative Board-Interviews, das Konzept der „Technological Frames“, System-Dynamics-Modellierung und eine anschließende Resonanzbefragung. Im Mittelpunkt der Diskussion stand die weiterführende Frage, wie Entscheidungsräume so gestaltet werden können, dass verborgene Dynamiken kollektiv sichtbar und besprechbar werden. Die Präsentation fasste diesen Perspektivwechsel prägnant zusammen: Der beobachtete Problemraum ist nicht notwendigerweise identisch mit der zugrunde liegenden Problemdynamik.

Zentrale Erkenntnisse

- **Mehr Information führt nicht automatisch zu besserer Governance.** Berichte, Expertise und Kennzahlen können einzelne Sachverhalte erhellen, ohne die dahinterliegenden dynamischen Zusammenhänge sichtbar zu machen.
- Boardmitglieder betrachten Cybersecurity durch unterschiedliche **Interpretationsrahmen**. Beruflicher Hintergrund, regulatorische Erfahrung, persönliche Erlebnisse und Rollenverständnisse beeinflussen, was als relevant wahrgenommen und auf die Agenda gebracht wird.
- Der im Board diskutierte Problemraum ist deshalb nicht identisch mit der zugrunde liegenden Problemdynamik. Bestimmte Beziehungen und Wirkungen bleiben außerhalb des gemeinsamen Aufmerksamkeitsraums.

- **Kurzfristig plausible Maßnahmen können langfristig problematische Folgen erzeugen.** Ein typisches Muster ist die Reaktion auf einen Cybervorfall durch punktuelle Investitionen, nach denen der unmittelbare Problemdruck sinkt, während strukturelle Ursachen vertagt werden.
- Die Untersuchung unterscheidet zwischen weitgehend etablierten Governance-Normen, unterschiedlich gelebten Praktiken sowie „hidden or contested dynamics“, die relevant sein können, aber noch nicht kollektiv anerkannt oder institutionalisiert sind.
- Für kollektive Entscheidungsfähigkeit ist nicht nur individuelle Expertise erforderlich. Boards benötigen **gemeinsame Repräsentationen von Feedback, Verzögerungen, Akkumulationen und indirekten Effekten.**
- Die Diskussion zeigte, dass formale Board-Gespräche nur eingeschränkt einem offenen „Dialog“ entsprechen. Machtverhältnisse, Rollen, Vertraulichkeit, Regulierung und institutionelle Erwartungen begrenzen, was gesagt und gemeinsam reflektiert werden kann.
- Cybersecurity kann als besonders anschauliches Beispiel einer breiteren Klasse komplexer Governance-Probleme verstanden werden: hohe Unsicherheit, begrenzte Messbarkeit, strategische Verantwortung bei operativer Distanz und erhebliche indirekte Wirkungen.

Resümee des Austauschs

Der Austausch verlagerte den Blick von der Frage „Hat das Board genügend Cybersecurity-Wissen?“ hin zu der Frage: „**Welche Dynamiken kann das Board überhaupt gemeinsam sehen und bearbeiten?**“ Damit wird Governance auch zu einem Sichtbarkeits- und Repräsentationsproblem. Die Teilnehmenden diskutierten insbesondere die Grenzen formalisierter Board-Kommunikation, die Rolle von Macht und Diversität, die Abgrenzung strategischer und operativer Verantwortung sowie Möglichkeiten einer indirekten Systemdiagnose über Einzelinterviews und rekonstruierte Deutungsmuster. Als weiterführende Perspektive entstand die These, dass die entwickelte Logik nicht auf Cybersecurity beschränkt ist, sondern auch für andere komplexe, schwer messbare Risikofelder relevant sein könnte.



Zentrale Themen des Austauschs

1. Vom Informationsdefizit zum Sichtbarkeitsproblem

- Übliche Governance-Debatten setzen häufig bei zusätzlicher Expertise, besseren Berichten oder mehr technischen Informationen an. Das Forschungsprojekt verschiebt den Fokus auf die Frage, **was im Entscheidungsraum tatsächlich sichtbar und anschlussfähig wird.**
- Technische, juristische oder regulatorische Erfahrungen prägen die Wahrnehmung einzelner Boardmitglieder. Cybersecurity wird dadurch nicht als einheitlicher Gegenstand behandelt, sondern durch unterschiedliche „Linsen“ interpretiert.
- Mehr Wissen über Einzelaspekte genügt daher nicht, wenn Feedbackschleifen, Verzögerungen und indirekte Effekte als Beziehungen zwischen diesen Aspekten unsichtbar bleiben. Die Präsentation fasst dies als Weg von Interpretation und Board-Dialog zur „Dynamic Governance Capability“.

2. Forschungslogik: von Board-Erfahrungen zu dynamischen Governance-Mechanismen

- Ausgangspunkt waren Interviews mit erfahrenen Boardmitgliedern zu Wahrnehmungen, Verantwortlichkeiten und Erfahrungen mit Cybersecurity-Governance.
- Aus den Interviewaussagen wurden „Technological Frames“ rekonstruiert. Anschließend wurden wiederkehrende Zusammenhänge mit System Dynamics als Rückkopplungsstrukturen, Verzögerungen und mögliche systemische Archetypen modelliert.
- Aus den dynamischen Mustern wurden Governance-Interventionen abgeleitet und in einer Befragung daraufhin geprüft, wie stark sie mit den Erfahrungen weiterer Boardmitglieder resonieren.
- Die Forschungslogik lautet damit: **Interviewaussagen → rekonstruierte Dynamiken → Governance-Interventionen → empirische Resonanz.** Insgesamt wurden 12 dynamische Schleifen (System Dynamics Loops), 26 Strategien und 23 Survey-Fragen entwickelt.

3. Kurzfristig plausible Maßnahmen können langfristig problematisch werden

- Als anschauliches Beispiel wurde das System-Dynamics-Muster „**Fixes that Fail**“ erläutert. Nach einem Cybervorfall reduziert eine kurzfristige Intervention zunächst den akuten Problemdruck.
- Mit sinkender Aufmerksamkeit werden weitergehende Maßnahmen jedoch vertagt; ungelöste Ursachen bleiben bestehen und erhöhen später erneut den Cyberdruck.
- Das Beispiel verdeutlicht, warum lokal rationale Entscheidungen im Zeitverlauf unerwünschte systemische Effekte erzeugen können. Gerade diese Dynamik ist im Moment der Einzelentscheidung häufig nicht sichtbar.

4. Welche Governance-Praktiken resonieren in Boards?

- Hohe Zustimmung bei vergleichsweise geringer Streuung zeigten unter anderem Board-Level-Cyberexpertise, kollektive Diskussion und Lernen aus Vorfällen. Diese Praktiken wurden als weitgehend **institutionalisierte Governance-Normen** eingeordnet.
- Andere Maßnahmen – etwa die Trennung strategischer und operativer Cyberthemen, langfristige Cyberinvestitionen oder der Fokus auf Detektion und Reaktion – wurden grundsätzlich positiv bewertet, aber unterschiedlich erlebt und umgesetzt.
- Besonders interessant sind Praktiken mit geringerem Konsens und hoher Varianz, darunter proaktives Agenda-Setting, kontinuierliches Lernen des Boards und Peer-Austausch. Sie können wichtige Hebelpunkte darstellen, sind aber noch nicht kollektiv etabliert.
- Die **Streuung der Antworten** ist damit selbst analytisch relevant: Sie zeigt, ob eine Praxis nicht nur Zustimmung findet, sondern auch gemeinschaftlich geteilt und institutionalisiert ist.

5. Was bedeutet „Dialog“ im Board?

- In der Diskussion wurde darauf hingewiesen, dass ein Board-Gespräch nicht mit einem offenen Dialog im Sinne dialogischer Kommunikationskonzepte gleichgesetzt werden sollte.
- Board-Kommunikation ist formalisiert und durch Agenda, Rollen, Vertraulichkeit, Regulierung, Unternehmenspolitik und Machtbeziehungen begrenzt. Bestimmte Themen oder Einschätzungen können bekannt sein, ohne im Kollektiv offen ausgesprochen zu werden.
- Gerade diese Differenz zwischen individueller Wahrnehmung und kollektiv Sagbarem macht die indirekte Rekonstruktion von Gesprächsdynamiken interessant.
- Für die Forschung entsteht daraus zugleich ein methodisches Problem: Die eigentlichen Sitzungen sind kaum direkt beobachtbar; untersucht werden daher Berichte, Erfahrungen und Deutungen der Beteiligten.

6. Strategische Verantwortung bei operativer Distanz

- Mehrere Beiträge beschäftigten sich mit der Frage, wie weit Boards bei Cybersecurity in operative Fragen einsteigen sollten. Operative Entscheidungen liegen grundsätzlich beim Executive Management.
- Aufsichtsräte und Boards tragen jedoch Verantwortung für Risikorichtung, Investitionen, Prioritäten und die Beurteilung strategischer Konsequenzen. Dazu benötigen sie genügend Verständnis, um Risiken beurteilen und Managemententscheidungen hinterfragen zu können.
- Die Herausforderung besteht darin, **strategische Urteilsfähigkeit aufzubauen, ohne in Mikromanagement zu geraten**. Gerade hier zeigten die Befragungsergebnisse unterschiedliche Erfahrungen und Rollenvorstellungen.

7. Wie lassen sich verborgene Dynamiken diagnostizieren?

- Als praktische Möglichkeit wurde eine indirekte Systemdiagnose diskutiert: Einzelinterviews können sichtbar machen, wie Akteure über ihre Organisation, andere Beteiligte und Problemlagen sprechen.
- Eine neutrale Zusammenführung solcher Aussagen kann Muster offenlegen, die in Gruppensituationen nicht artikuliert werden. Voraussetzung sind ein entsprechendes Mandat und Vertrauen in die Auswertung.
- Auch Zusammensetzung, Diversität, Branchenkontext und Machtverteilung im Board wurden als mögliche Einflussgrößen angesprochen. Diese Aspekte wurden im vorgestellten Projekt nicht systematisch quantitativ untersucht, bieten aber Ansatzpunkte für weitere Analysen.
- Damit entsteht eine Verbindung zur kybernetischen Beobachtung: Nicht nur Entscheidungen selbst, sondern auch die **Bedingungen ihrer Beobachtbarkeit und Besprechbarkeit** werden zum Gegenstand der Analyse.

8. Cybersecurity als Beispiel einer breiteren Klasse komplexer Governance-Probleme

- In der Schlussdiskussion wurde gefragt, ob Cybersecurity weniger ein Sonderfall als vielmehr ein besonders deutliches Beispiel für komplexe, schwer beobachtbare Governance-Probleme ist.
- Als Besonderheiten wurden die hohe Unsicherheit, der „Nicht-Ereignis“-Charakter erfolgreicher Prävention und insbesondere das Fehlen einer allgemein anerkannten Metrik für Cybersecurity diskutiert.
- Cybersecurity erscheint auf Board-Ebene zudem häufig über Stellvertreter wie Risikomanagement, Compliance, Investitionen oder Haftung. Die zugrunde liegende technische Realität bleibt damit teilweise indirekt.
- Die vorgestellte Forschungslogik könnte deshalb auch für andere Themen interessant sein, bei denen Entscheider strategische Verantwortung tragen, obwohl der Gegenstand nur unvollständig messbar und nicht unmittelbar beobachtbar ist.

Literatur:

Rehm, Sven-Volker; Georg Schaffner, Laura; and Goel, Lakshmi, "Framing Dialogues on Cyber-Resilience on Boards" (2021). *ICIS 2021 Proceedings*. 10. https://aisel.aisnet.org/icis2021/is_resilience/is_resilience/10

Podcast: AIS Insights. <https://ais-insights.ai/insights/756>

Hinweis zur Entstehung dieses Protokolls

Dieses Protokoll wurde auf Basis einer automatisierten Transkription der Online-Veranstaltung und einer anschließenden thematischen Strukturierung durch ein Sprachmodell erstellt. Ziel war es, die zentralen Inhalte und Diskussionsthemen für eine breitere Nachnutzung zugänglich zu machen. Die Durchsicht durch Beteiligte bestätigte eine im Wesentlichen korrekte und sachgerechte Wiedergabe des Gesprächsverlaufs. Es handelt sich dennoch nicht um ein autorisiertes Wortprotokoll, sondern um eine strukturierte Zusammenfassung, die den Charakter des offenen Gesprächsformats berücksichtigt.

Für weitere Informationen zu Inhalt, Referenten oder Folgeveranstaltungen besuchen Sie synergylab.space oder wenden Sie sich gerne an die Gesellschaft für Wirtschafts- und Sozialkybernetik e.V. unter office@gws-kybernetik.org.