Christina Gräfin von Wintzingerode, Dirk Müllmann und Prof. Dr. Indra Spiecker gen. Döhmann

Neue Strukturen in der Europäischen Cybersicherheit – ein Über- und Ausblick

Mit der Verordnung (EU) 2021/887 zur Errichtung des Europäischen Kompetenzzentrums für Industrie Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Kompetenzzentren hat die Europäische Union neue Strukturen geschaffen, um die Vernetzung und den Austausch zwischen den Mitgliedsstaaten im Bereich der IT-Sicherheit zu verbessern. Nach einer ersten Konstituierungsphase haben die neuen Institutionen nun ihre Arbeit aufgenommen. An Herausforderungen mangelt es nicht – ob der gesetzliche Auftrag und die Organisation des Netzwerks und seiner Akteure das aber ermöglichen, erscheint fraglich.

Cybersicherheit in Europa

Russlands Einmarsch in die Ukraine im Februar 2022 wurde von einer Vielzahl digitaler Angriffe auf die Infrastruktur des Landes sowie der Mitgliedsstaaten von EU und NATO begleitet (vgl. nur Microsoft, Microsoft Digital Defense Report 2022, S. 2). Und auch abseits dieser kriegerischen Auseinandersetzung nimmt die Bedrohungslage für die IT-Sicherheit in Deutschland in allen Bereichen kontinuierlich zu (vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2022, S. 8.). Die öffentliche Verwaltung, Kliniken und Universitäten, aber auch Unternehmen und Privatleute sehen sich immer häufiger Attacken auf ihre IT-Systeme ausgesetzt, die – sind sie erfolgreich – zum Ausfall von Dienstleistungen und Wertschöpfung führen. Vor diesem Hintergrund werden Cyberangriffe in der Bevölkerung zunehmend als reale und unmittelbare Bedrohung des eigenen Alltags wahrgenommen, mit denen staatliche oder private Akteure mit einfachen Mitteln wesentliche Infrastrukturen und damit die Funktionsfähigkeit der Gesellschaft beeinträchtigen können.

Die Europäische Union hat sich der Cybersicherheit als Zukunftsthema schon früh angenommen und, zum Beispiel bereits 2004 mit der Einrichtung der Agentur für Cybersicherheit (ENISA), Maßnahmen zur unionsweiten Verbesserung des IT-Sicherheitsniveaus in Europa ergriffen. Mit der noch relativ neuen und unbekannten Verordnung (EU) 2021/887 zielt sie nun darauf ab, dass die relevanten Akteure im Bereich der Cybersicherheit ermächtigt werden, sich mit ihrem Fachwissen und ihren Erfahrungen zu vernetzen. Hierdurch soll die Fragmentierung der Anstrengungen zur Forschung an und Entwicklung von IT-Sicherheitsprodukten in der EU beendet sowie der europäische IT-Sicherheitsstandort gestärkt und weiterentwickelt werden. Zugleich zielt das Netzwerk auf eine bessere Verknüpfung der Akteure in der Praxis mit der Politik und den dort zu fällenden Entscheidungen ab. Das vorhandene Fachwissen, insbesondere in der Forschung zur IT-Sicherheit, soll zukünftig auch in bedarfsgerechte und marktfähige Produkte überführt werden, um so die Abhängigkeit von außereuropäischen IT-Produkten zu verringern.

Ob gerade das Ziel der Vernetzung und Einbindung der Community in politische Entscheidungen auf Basis der im Juni 2021 in Kraft getretenen Verordnung erreicht werden kann, erscheint angesichts der getroffenen gesetzlichen Entscheidungen offen. Die neu geschaffenen Institutionen auf europäischer und nationaler Ebene werden sich umfassend engagieren müssen, damit das avisierte Netzwerk nicht nur eine teure Doppelstruktur wird.

Die Regelungen der Verordnung

Die Umsetzung der in der Verordnung festgesetzten Ziele durch das Netzwerk obliegt drei Akteuren. Die zentrale Rolle kommt dabei dem europäischen Kompetenzzentrum für Cybersicherheit zu, das für die Koordination der IT-sicherheitsrelevanten Aktivitäten auf europäischer und nationaler Ebene ebenso zuständig ist wie für die Planung und Umsetzung von Forschungs- und Entwicklungsaufgaben im Bereich der Cybersicherheit sowie die Beratung und Unterstützung der damit befassten Akteure in der EU. Eine zweite Gruppe von Beteiligten, und zwar auf Ebene der Mitgliedsstaaten, sind die nationalen Koordinierungszentren, deren Aufgabe in der Unterstützung und Förderung des Kompetenzzentrums und der Mitglieder der Cybersicherheitsgemeinschaft, der dritten Gruppe von Akteuren, liegt. Die Koordinierungszentren fungieren als Anlaufstellen und stellen Hilfe in Form von Finanzmitteln, Fachwissen und technischer Unterstützung bereit. Die Aufgabe der zuvor genannten Kompetenzgemeinschaft für Cybersicherheit liegt in der Unterstützung des Kompetenzzentrums und des Netzwerks bei deren Projekten sowie der Entwicklung und Verbreitung von Fachwissen im Bereich der IT-Sicherheit. Der Mitgliederkreis ist dabei bewusst offengehalten und soll die wichtigsten Interessenträger zusammenbringen. Das sind einerseits Einrichtungen aus Industrie, Wissenschaft und Forschung, Organisationen der Zivilgesellschaft, aber auch Normungsorganisationen und öffentliche oder private Einrichtungen, die sich mit Cybersicherheit befassen, sowie Akteure aus anderen Bereichen, die ein Interesse an Cybersicherheit haben oder sich damit verbundenen Herausforderungen stellen müssen. Die Zugehörigkeit zur Gemeinschaft wird vom Kom-

petenzzentrum und den nationalen Koordinierungszentren reguliert.

"Top-Down" statt "Bottom Up"

Der europäische Gesetzgeber hat für die Steuerung und Zusammenarbeit der verschiedenen Gruppen von Akteuren einen top-down Ansatz gewählt. Diese auf Anordnungen und Kontrolle basierende Steuerungsstruktur ermöglicht schnelle Reaktionen und das Treffen verbindlicher Entscheidungen, vorausgesetzt, dass die Entscheidungsträger über ausreichende zeitliche Ressourcen und das für die Entscheidungen notwendige Wissen verfügen. Während die Einbindung öffentlicher Akteure in eine Top-down-Struktur zumeist wegen ihrer ohnehin bestehenden Bindungen durch das Demokratie- und das Rechtsstaatsprinzip einfach zu etablieren sein dürfte, stellt sich dieser Ansatz für die Integration der Kompetenzgemeinschaft als wenig tauglich dar. Selbst wenn die Kompetenzgemeinschaft gemäß der Definition in der Verordnung auch öffentliche Akteure umfasst, dürfte die Gruppe privater Akteure doch den ganz überwiegenden Teil möglicher Mitglieder darstellen. Um diese zu erreichen und dazu zu motivieren, ihre Expertise und Erfahrungen auf dem Gebiet der Cybersicherheit in die von der Verordnung geschaffene Struktur einzubringen, ist der Weg des „command-and-control" ungeeignet. Sie unterliegen keinen öffentlich-rechtlichen Bindungen, d.h. private Akteure müssen für sich einen eigenen Anreiz oder Mehrwert darin sehen, sich freiwillig einzubringen. Diesen kann ein reiner top-down Ansatz nicht bieten. Die Möglichkeit, auch Bottom-up-Strukturen in die Verordnung einzubringen, hat der Gesetzgeber verpasst. Nicht zuletzt wäre das in einem solchen Ansatz liegende Potenzial als Sammelbecken für Fachwissen, für die Wissensbeschaffung und -verteilung sowie die Aktivierung von Forschungs- und Entwicklungskapazitäten den Zielen der Verordnung dienlich gewesen, abgesehen davon, dass man damit die echten Bedarfe hätte einfacher und auf breiterer Basis identifizieren können.

Begrenzter Aufgabenbereich und fehlende Einflussmöglichkeiten

Der Kompetenzgemeinschaft kommt die Aufgabe zu, Fachwissen auf dem Gebiet der Cybersicherheit in der gesamten Union zu fördern, zu teilen und zu verbreiten sowie das Kompetenzzentrum und das Netzwerk bei der Erfüllung ihrer Aufgaben zu unterstützen (Art. 8 Abs. 1, 9 VO (EU) 2021/887). Nimmt man diese Aufgabenstellung ernst, dann überrascht die begrenzte Rolle, die die Verordnung der Kompetenzgemeinschaft zuweist.

Im Europäischen Kompetenzzentrum ist die Gemeinschaft nur an wenigen Stellen eingebunden. Ihre Mitglieder können als Beobachter zu Sitzungen des Verwaltungsrats im Europäischen Kompetenzzentrum eingeladen werden, einen permanenten Beobachterstatus oder ein Stimmrecht haben sie jedoch nicht (Art. 12 Abs. 6, 14 Abs. 5 VO (EU) 2021/887).

Darüber hinaus ist eine strategische Beratungsgruppe (Art. 18 ff. VO (EU) 2021/887), bestehend aus höchstens 20 Vertretern der Mitglieder der Kompetenzgemeinschaft als Teil der Organisationsstruktur des Kompetenzzentrums vorgesehen. Doch auch der Beratungsgruppe kommt weder ein Stimmrecht noch ein Beobachterstatus im Verwaltungsrat zu. Ihre Empfehlungen sind nicht bindend und Abweichungen oder gar ihre Nichtberücksichtigung bei Entscheidungen des Verwaltungsrats unterliegen keiner Begründungspflicht.

Neben der mit eigenen Aufgaben versehenen strategischen Beratungsgruppe können durch den Verwaltungsrat bei Bedarf Arbeitsgruppen gebildet werden, um an Fragen, die für die Arbeit des Kompetenzzentrums von Bedeutung sind, mitzuarbeiten (Art. 13 Abs. 3 lit. n i.V.m. Art. 8 Abs. 9, 9 lit. b VO (EU) 2021/887).

In allen genannten Fällen hat die Kompetenzgemeinschaft selbst kein Mitbestimmungsrecht, welche ihrer Mitglieder als Beobachter, Teil der strategischen Beratungsgruppe oder in den Arbeitsgruppen teilnehmen. Die Verordnung verfolgt also ersichtlich kein Konzept zur Repräsentation der Kompetenzgemeinschaft im Europäischen Kompetenzzentrum. Die Gemeinschaft kann weder selbst gewählte Vertreter dorthin entsenden noch wirksam ihre Interessen, Forschungs- oder Entwicklungsergebnisse einbringen.

In den Strukturen der nationalen Koordinierungszentren sind für die Mitglieder der Kompetenzgemeinschaft keine Aufgaben vorgesehen, jedoch enthält die Verordnung immerhin Regelungsansätze für ihre Zusammenarbeit (Art. 3 Abs. 2, 7 Abs. 1 sowie Art. 8 Abs. 2 Satz 3, 9 lit. a, lit. c VO (EU) 2021/887). Die Ausgestaltung der nationalen Koordinierungszentren als Anlaufstellen für die Gemeinschaft auf mitgliedstaatlicher Ebene einerseits und der Auftrag an die Gemeinschaft andererseits, die nationalen Zentren in ihre Arbeit einzubeziehen, schafft zwar auch hier weder Repräsentation noch Einfluss, aber doch wenigstens größere Schnittstellen als im Kompetenzzentrum. Die Umsetzung und der Erfolg der Zusammenarbeit werden jedoch wesentlich von den einzelnen nationalen Koordinierungszentren abhängen, worin Chancen und Risiken zugleich liegen. Die Koordinierungszentren sind unterschiedlich gut organisiert und ausgestattet und auch die Kompetenzgemeinschaft ist nicht homogen über die Mitgliedstaaten verteilt. Nicht übersehen werden darf jedenfalls, dass ein gleichmäßig hohes Niveau der Cybersicherheit in allen Mitgliedstaaten der Europäischen Union auf diese Weise weder kurz- noch mittelfristig erreicht werden wird.

Hindernisse auf dem Weg zur Entstehung der Kompetenzgemeinschaft

Auch das Konzept der Kompetenzgemeinschaft selbst birgt Hindernisse, die für eine stabile Etablierung erst noch überwunden werden müssen. Ziel der Verordnung ist es, möglichst viele betroffene Bereiche und vorhandene Kompetenzen auf dem Gebiet der Cybersicherheit abzudecken. Das bedingt zugleich, dass sich in der Gemeinschaft auch Wettbewerber mit gegenläufigen Interessen hinsichtlich Marktanteilen, Wettbewerb um Fördermittel oder politischen Einfluss begegnen werden. Es wäre optimistisch, anzunehmen, dass sich daraus automatisch eine Gemeinschaft bildet, die ein gemeinsames Ziel verfolgt, harmonisch interagiert, ihr Wissen teilt und kooperiert.

Eine Organisationsstruktur, wie sie die Verordnung für das Europäische Kompetenzzentrum vorsieht und wie sie die nationalen Koordinierungszentren als öffentliche Einrichtungen nach mitgliedstaatlichem Recht erhalten, steht der Kompetenzgemeinschaft nicht zur Verfügung. Für ihre Etablierung kann also nicht einfach auf ein bewährtes Modell zurückgegriffen werden.

Berücksichtigt werden muss außerdem, dass nicht alle Mitglieder der Gemeinschaft über die notwendigen finanziellen und personellen Ressourcen verfügen dürften, die z. B. eine effektive und gleichberechtigte Mitwirkung in der Struktur des Europäischen Kompetenzzentrums erfordert. Das Konzept der Kompetenzgemeinschaft trägt zumindest in dieser Hinsicht Züge eines exklusiven Partizipationsmodells, das dem erklärten Ziel der Einbindung von KMU und Start-Ups ersichtlich entgegensteht und von vornherein nicht allen Interessen die gleichen Durchsetzungschancen ermöglicht. Damit gehen aber auch Potenzial, Expertise und Erfahrungen dieser Interessenträger für die Gemeinschaft und die europäische Cybersicherheit insgesamt verloren. Ganz abgesehen davon, dass damit gerade diejenigen Akteure gestärkt werden, die schon jetzt oftmals aufgrund ihrer Größe und Bedeutung von rechtlichen Regeln schwer zu steuern sind.

Wie kann es dennoch gelingen?

Gemessen an den Zielen der Verordnung ist die Kompetenzgemeinschaft mit ihren Mitgliedern in Anbetracht des dort vorhandenen Fachwissens und des Forschungs- und Entwicklungspotenzials der entscheidende Erfolgsfaktor für die Cybersicherheit in der Europäischen Union. Die Rolle, die der Gemeinschaft zuerkannt wird, spiegelt dies jedoch nicht wider.

Um dennoch sowohl die fehlende Anreizstruktur für potenzielle Gemeinschaftsmitglieder als auch die Hindernisse auf dem Weg der Gemeinschaftsbildung möglichst schnell überwinden zu können, wird es maßgeblich auf die Arbeit der nationalen Koordinierungszentren ankommen. Als Anlaufstellen dürfen sie nicht nur punktuell den Kontakt mit der Kompetenzgemeinschaft suchen, wie dies im Kompetenzzentrum der Fall ist. Die Koordinierungszentren sollten deshalb nicht nur in Frage kommende Mitglieder identifizieren und ansprechen, sondern insbesondere auch bereits existierende, gut etablierte Netzwerke in den Blick nehmen. Die Integration solcher Netzwerke in die Kompetenzgemeinschaft lässt diese nicht nur zahlenmäßig schnell anwachsen, sondern mit den Netzwerken werden zugleich schon erprobte Organisationsstrukturen integriert, die dem Konzept der Kompetenzgemeinschaft in der Verordnung wie gesehen bislang vollständig fehlen. Gleichzeitig besteht innerhalb etablierter Netzwerke bereits ein gewisses Maß an gegenseitigem Vertrauen sowie Erfahrungen in der Zusammenarbeit. Nicht zuletzt bieten die Netzwerke auch insofern einen Mehrwert, dass sie durch ihre Aktivitäten die Sichtbarkeit der Kompetenzgemeinschaft erhöhen und auf diesem Weg weitere künftige Mitglieder erreicht und integriert werden können.

Aber auch, oder gerade, etablierte Netzwerke und deren Mitglieder brauchen Anreize, sich in die Kompetenzgemeinschaft einzubringen. Ziel des Europäischen Kompetenzzentrums und der nationalen Koordinierungszentren muss es darum sein, diese Netzwerke schnell zu integrieren und zu unterstützen, um die dort bereits stattfindende Arbeit zu fördern und einen weiteren und intensiveren Austausch zu ermöglichen.