Ein Netzwerk für Europas Cybersicherheit

Wiss. Mitarbeiterin Ref. jur. Christina Gräfin von Wintzingerode, Wiss. Mitarbeiter Dirk Müllmann und Professorin Dr. Indra Spiecker gen. Döhmann, LL. M.*

Der Beitrag befasst sich mit dem Verordnungsentwurf 2018/0328/ (EU) der Europäischen Kommission zur Einrichtung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung und eines Netzes nationaler Koordinierungszentren. Nach einem Überblick über die vorgesehene Netzwerkstruktur werden die rechtlichen Herausforderungen der Gestaltung eines europäischen Netzwerkes herausgearbeitet. Welche Akteure sollten eingebunden werden und wie kann dies sinnvoll geschehen? Welche Anforderungen sind an das Steuerungskonzept für das Kompetenznetzwerk im Lichte europäischer Werte zu stellen? Und in welchem Verhältnis soll das künftige Netzwerk zur ENISA stehen?

I. Einleitung

Digitale Technologien nehmen angesichts ihrer steigenden Einbindung im Alltag immer mehr Einfluss auf Wirtschaft und Gesellschaft. Die damit ebenso wachsende Abhängigkeit vom Funktionieren der Technologie und die steigende Vulnerabilität der Gesellschaft bei ihrem Ausfall sind vor dem Hintergrund der grenzenlosen Netze und Lieferketten längst kein nationales Thema mehr, sondern eine Frage europäischer Unabhängigkeit. Derzeit hängt die IT-Sicherheit der Union als Nettoimporteurin von Cybersicherheitsprodukten und -lösungen allerdings weitgehend von nichteuropäischen Anbietern ab.[1] Dies schmälert sowohl die Wettbewerbsfähigkeit des europäischen Binnenmarkts als auch die Fähigkeit der Union zur Eigensicherung ihrer digitalen Werte und Anlagen. Gleichzeitig ist jedoch in den Mitgliedstaaten der Union eine Fülle von Fachwissen und Erfahrungen zu Fragen der Cybersicherheit vorhanden.[2] Weshalb also spielt Europa auf dem Cybersicherheitsmarkt nur eine so untergeordnete Rolle? Als Ursachen hierfür wurden fragmentierte Anstrengungen in Forschung und Industrie identifiziert, denen es an Einheitlichkeit und einer gemeinsamen europäischen Zielrichtung mangelt.[3] Ein europäisches Netzwerk für Cybersicherheit soll hier künftig Abhilfe schaffen.

II. Rechtliche Herausforderungen einer europäischen Netzwerkgestaltung

Das im Entwurf skizzierte Netzwerk soll europaweit Akteure aus unterschiedlichen Disziplinen zusammenbringen, um die bestehenden Anstrengungen in Forschung und Industrie und das dort vorhandene Fachwissen zu bündeln und effizient nutzen zu können.[4] Die Erreichung dieses Ziels wird wesentlich von der erfolgreichen Kooperation der beteiligten Akteure abhängen. Insofern stellen sich Fragen nach dem rechtlichen Rahmen für die Kooperation an sich ebenso wie danach, welchen rechtlichen Anforderungen die späteren Handlungen des Netzwerks genügen müssen.

1. Kooperationsformen öffentlicher und privater Akteure

Die rechtlichen Rahmenbedingungen einer europäischen Kooperation hängen von verschiedenen Faktoren ab, wobei der wichtigste die Akteure selbst sind. Die Einbindung und jeweilige Rolle privater (zB Unternehmen, Forschungseinrichtungen) und öffentlicher (zB Europäische Kommission, Behörden in den Mitgliedstaaten) Akteure ist entscheidend für die Anforderungen an die rechtlichen

Grundlagen ihrer Zusammenarbeit.

Während für die Kooperation von Privaten im europäischen Binnenmarkt sowohl im Vertrags- als auch im Gesellschaftsrecht etablierte Regelungsmodelle vorhanden sind, fällt der Befund für gemischte oder rein öffentliche Kooperationsmodelle deutlich anders aus. Bereits auf mitgliedstaatlicher Ebene gibt es kaum Regelungen für solche Kooperationsmodelle.[5] Auf Unionsebene fehlen detaillierte Regelungen für die rechtlichen Strukturen dieser Kooperationen ganz. Zwar ist grundsätzlich denkbar, auch für die Kooperation mit oder zwischen öffentlichen Institutionen vertragliche Modelle heranzuziehen, aber nicht jede Form der Kooperation ist rechtlich relevant und bedarf gegenseitiger vertraglicher Bindungen, wie sie beispielsweise ein Leistungsaustausch erforderlich macht. Zum anderen besteht eine Gestaltungsfreiheit, wie sie Privaten durch die Vertragsfreiheit zukommt, für öffentliche Institutionen gerade nicht. Sie unterliegen in ihrem Handeln den Bindungen und Begrenzungen des Demokratie-[6] und des Rechtsstaatsprinzips,[7] die beide auch grundlegende europäische Prinzipien[8] darstellen.

Auch der Gedanke, das Netzwerk als Europäische Agentur wie etwa ENISA oder ECHA zu gestalten, trägt bei näherer Betrachtung nicht. Agenturen sind von den Europäischen Institutionen gegründete selbstständige Verwaltungseinheiten, deren Rechtsgrund jeweils in einem konkreten Sekundärrechtsakt liegt.[9] Als Sonder- oder Fachbehörden dienen sie der Wahrnehmung spezieller Aufgaben.[10] Das Netzwerk für Cybersicherheit dagegen besitzt eine solche Zuweisung von Verwaltungsaufgaben ausweislich des Verordnungsentwurfs nicht und auch die Grundidee eines Netzwerks aus privaten und öffentlichen Einrichtungen widerspricht einer Ausgestaltung als Europäische Agentur.

> Gräfin von Wintzingerode/Müllmann/Spiecker gen. Döhmann: Ein Netzwerk für Europas Cybersicherheit

Insgesamt lässt sich feststellen, dass die Schaffung eines europäischen Netzwerks eines komplexen Regelungsrahmens bedarf, der jedoch in der bestehenden europäischen Rechtsordnung so nicht existiert. Aus diesem Befund ergibt sich somit eine wichtige Anforderung: Mangels Vorlage für den Regelungsrahmen muss die Verordnung die Steuerungsstrukturen für die Kooperation verschiedenster Akteure im Netzwerk selbst schaffen. Inwieweit dies im Vorschlag der Kommission bereits der Fall ist, wird unter III. näher betrachtet.

2. Aktivitäten des künftigen Netzwerks

Mit der Förderung der Cybersicherheit ist dem Netzwerk eine breite Aufgabenstellung angedient, die Raum für vielfältige Aktivitäten im Bereich der Forschung, Entwicklung und Bildung lässt. Für konkrete Aktivitäten des Netzwerks ergeben sich bereichsabhängig spezifische, materiell-rechtliche Fragen, die, um nur einige Beispiele zu nennen, vom Vergaberecht über die Geheimhaltung von Betriebs- und Geschäftsgeheimnissen bis hin zu Berührungen mit dem Bildungs- oder Hochschulrecht in den Mitgliedstaaten reichen können. Es entstehen also vielfältige Wechselwirkungen zwischen der Aufgabenzuweisung innerhalb des Netzwerks, seinen Kooperationsformen, Handlungen nach außen und dem materiellen Recht. Inwieweit Entscheidungen des Netzwerks oder seiner Teile also wirksam möglich oder Handlungen rechtmäßig sind, ist jeweils eine Frage des konkreten Einzelfalls.

3. Kompetenzen der EU

Nach dem Prinzip der begrenzten Einzelermächtigung in Art. 5 II EUV wird die Europäische Union nur in den Grenzen der Zuständigkeiten tätig, die ihr in den Verträgen von den Mitgliedstaaten übertragen wurden. Den Verträgen muss sich also eine Kompetenzgrundlage für den Erlass einer europäischen Verordnung entnehmen lassen,[11] um das Cybersicherheitsnetzwerk zu schaffen.

Der Verordnungsvorschlag wird auf Art. 173 III, 188 I AEUV gestützt, wobei Letzterer auf Art. 187 AEUV verweist, der die Gründung gemeinsamer Unternehmen und Strukturen zur Durchführung von Forschungs- und technologischen Entwicklungsprogrammen zum Gegenstand hat. Grundsätzlich lässt sich die Idee der Schaffung eines Netzwerks für Cybersicherheit in Industrie, Technologie und Forschung darunter fassen. Fragen ergeben sich aber hinsichtlich der zu wählenden Rechtsform des Kompetenzzentrums und der rechtlichen Ausgestaltung der Zusammenarbeit des Netzwerks sowie der Reichweite der Unionskompetenz hinsichtlich der konkreten Aufgaben, wie sie der Verordnungsentwurf vorsieht. Im weiteren Verlauf des Gesetzgebungsprozesses sollte hierauf besonderes Augenmerk gelegt werden.

III. VO-Entwurf (EU) 2018/0328

Nachfolgend soll der Verordnungsentwurf einer kritischen Betrachtung unterzogen werden. Soweit nicht anders gekennzeichnet, handelt es sich bei den Artikelangaben um solche des Entwurfs.

1. Gesetzgebungsprozess

Im Bereich der Sicherheit von Netz- und Informationssystemen ist die EU seit langem gesetzgeberisch aktiv und macht das Thema im kommenden Rahmenprogramm „Horizont Europa"[12] sogar zu einer Priorität.[13] Zurückgehend auf eine gemeinsame Mitteilung der Kommission mit der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik, eine Aufforderung der Staats- und Regierungschefs und Schlussfolgerungen des Rates im Jahr 2017 entwickelte die Kommission den vorliegenden Entwurf der VO (EU) Nr. 2018/0328.[14] Er dient als ein erster Schritt zur Umsetzung des Programmes „Digitales Europa"[15] und wurde am 12.9.2018 durch die Europäische Kommission angenommen.[16] Im Zuge des seither laufenden Gesetzgebungsprozesses wurden vom Europäischen Wirtschafts- und Sozialausschusses zwei Stellungnahmen zu dem Entwurf vorgelegt.[17] Zudem hat das Europäische Parlament nach der ersten Lesung des Entwurfs eine Stellungnahme mit einer Vielzahl von Änderungsanträgen abgegeben.[18] Auch im Rat befindet sich der Vorschlag seither in der ersten Beratungsrunde.

2. Vorgesehene Institutionen

Das wesentliche Ziel der Verordnung besteht in der Schaffung eines Europäischen Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung, der Einrichtung eines Netzes von nationalen Koordinierungszentren sowie der Entwicklung der Grundlagen für die Errichtung einer Kompetenzgemeinschaft für Cybersicherheit in Europa (Art. 1 I). Unter Cybersicherheit wird dabei der „Schutz von Netz- und Informationssystemen, deren Nutzern und sonstigen Personen vor Cyberdrohungen" (Art. 2 I) verstanden.

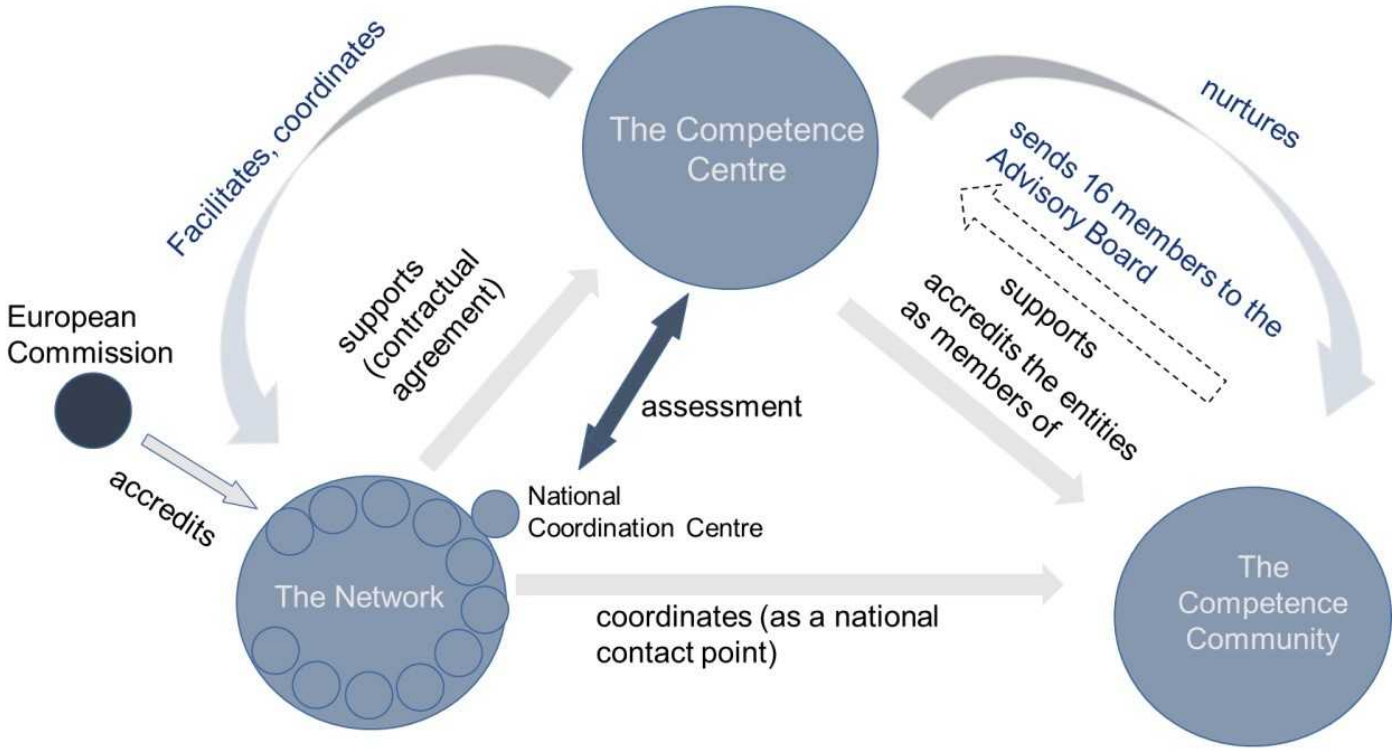

Abb. 1: Vorgesehene Struktur des Europäischen Netzwerks und Aufgaben der Akteure. [19]

a) Kompetenzzentrum

Kern der geplanten neuen europäischen Cybersicherheitsarchitektur ist das Europäische Kompetenzzentrum für Cybersicherheit in Industrie, Technologie und Forschung. Es soll als eigenständige, rechts- und geschäftsfähige Rechtsperson (Art. 1 IV) die Union bei der Wahrung und Weiterentwicklung der Cybersicherheitskapazitäten ebenso wie bei der Steigerung der Wettbewerbsfähigkeit der Cybersicherheitsbranche in Europa unterstützen (Art. 3).

Gräfin von Wintzingerode/Müllmann/Spiecker gen. Döhmann: Ein Netzwerk für Europas Cybersicherheit

aa) Aufgaben, Struktur und Finanzierung

Die Aufgaben des Kompetenzzentrums leiten sich aus den im Verordnungsvorschlag definierten Zielen ab. So soll es die Koordinierung der Arbeiten des Netzes nationaler Koordinierungszentren und der Kompetenzgemeinschaft erleichtern, unterstützen und zugleich zur Umsetzung der in den Programmen der Union vorgesehenen Maßnahmen mit Bezug zur Cybersicherheit beitragen (Art. 4 I, II). Durch die Bereitstellung von Fachwissen und technischer Unterstützung sowie den Erwerb und die Unterstützung beim Erwerb von moderner industrieller und Forschungsinfrastruktur sollen ferner die Kapazitäten, das Wissen und die Infrastruktur im Bereich der Cybersicherheit verbessert werden (Art. 4 III). Das Zentrum soll einen Beitrag bei der Einführung moderner Cybersicherheitsprodukte und -lösungen leisten, indem es die Forschung, Entwicklung und Verbreitung fördert und

Unterstützung bei der Einführung und Integration, aber auch der Auftragsvergabe und Markterschließung leistet (Art. 4 IV). Es soll das Verständnis und die Qualifikation im Bereich der Cybersicherheit verbessern, indem es die Entwicklung von Cybersicherheitskompetenzen unterstützt (Art. 4 V). Außerdem soll das Zentrum mittels finanzieller Unterstützung, der Förderung von Großprojekten und der Unterstützung im Bereich der Normung einen Beitrag zur Stärkung der Cybersicherheitsforschung und -entwicklung in der EU leisten (Art. 4 VI). Weitere Ziele bestehen in der verbesserten Zusammenarbeit zwischen zivilen und militärischen Fachkreisen im Bereich der Cybersicherheit sowie der Schaffung von Synergien zwischen ihren zivilen und militärischen Dimensionen. Gemäß Art. 5 zählt zudem die Regelung des Betriebs und des Zugangs zu geförderten Infrastrukturen sowie die Möglichkeit der Durchführung von Vergabeverfahren zu den Aufgaben des Zentrums.

Die Mitgliedstaaten und die EU, vertreten durch die Kommission, sind die Mitglieder des Kompetenzzentrums, die seine Arbeit finanzieren (Art. 21 ff.). Seine Organisationsstruktur umfasst gem. Art. 11 einen Verwaltungsrat, einen Exekutivdirektor und einen wissenschaftlich-technischen Beirat.

Der Verwaltungsrat setzt sich aus je einem Vertreter pro Mitgliedstaat und fünf Kommissionsvertretern zusammen, die für vier Jahre ernannt werden (Art. 12). Er tagt mindestens dreimal jährlich unter Beteiligung des nicht stimmberechtigten Exekutivdirektors und, auf Einladung des Vorsitzes, von Mitgliedern des ebenfalls nicht stimmberechtigten wissenschaftlich-technischen Beirats (Art. 14). Er ist verantwortlich für die Ausrichtung sowie die Geschäfte des Zentrums und beaufsichtigt die Durchführung seiner Tätigkeiten (Art. 13 I). Zu seinen Aufgaben zählt unter anderem die Annahme von Strategie- und Arbeitsplänen, einer Finanzordnung, des Haushaltsplans sowie der Jahresabschlüsse und Bilanzen des Zentrums. Er entscheidet über die Verfahren zur Berufung eines Exekutivdirektors, den er ernennen und abberufen kann, über Kriterien und Verfahren der Einrichtung der Kompetenzgemeinschaft, die Einrichtung von Arbeitsgruppen sowie die Ernennung des wissenschaftlich-technischen Beirats (Art. 13 III). Die Entscheidungen des Verwaltungsrats ergehen mit doppelter Dreiviertelmehrheit, wobei der Union die Hälfte aller Stimmrechte eingeräumt sind, und jedem Mitgliedstaat eine Stimme zukommt (Art. 15 I–III).

Der Exekutivdirektor wird auf Vorschlag der Kommission vom Verwaltungsrat für vier Jahre ernannt und kann höchstens zwei Amtszeiten bekleiden (Art. 16). Als gesetzlicher Vertreter des Kompetenzzentrums ist er für das Tagesgeschäft und die Geschäftsführung zuständig, wobei er seine Befugnisse unabhängig wahrnimmt, gegenüber dem Verwaltungsrat aber rechenschaftspflichtig ist (Art. 17 I). Zu seinen Aufgaben gehören unter anderem die Unterstützung der Arbeit und Durchführung der Beschlüsse des Verwaltungsrats, die Entwicklung von Strategie, Arbeits- und Haushaltsplänen, die Durchführung des Arbeitsplans sowie diverse Verwaltungsaufgaben (Art. 17 II).

Der wissenschaftlich-technische Beirat tritt mindestens zweimal im Jahr zusammen und besteht aus maximal 16 Mitgliedern, die vom Verwaltungsrat aus den Reihen der Kompetenzgemeinschaft für Cybersicherheit für drei Jahre ernannt werden (Art. 18, 19 I). Ihm kommt die Organisation öffentlicher Konsultationen sowie die Beratung des Verwaltungsrats und des Exekutivdirektors zu, zB bei der Einsetzung von Arbeitsgruppen oder der strategischen Planung, wobei er zur Ausarbeitung des Arbeitsplans beiträgt und den Plan betreffendes Feedback fördert (Art. 19 II, 20).

bb) Kritik

Betrachtet man die Zusammensetzung des Verwaltungsrats, scheint zunächst eine hohe Gewichtung der Mitgliedstaaten gegenüber der Union vorzuliegen. Bei genauerer Betrachtung wird die hohe Repräsentanz der Mitgliedstaaten jedoch durch die Stimmengewichtung bei Entscheidungen

des Verwaltungsrats relativiert. Mit 50 % der Stimmen kommt der Kommission als Unionsvertreterin ein überproportional hoher Stimmanteil zu. Aufgrund der für alle Entscheidungen des Verwaltungsrats notwendigen Mehrheit von 75 % der Stimmen hat sie de facto ein Vetorecht. Das zusätzliche Erfordernis, dass die Stimmenmehrheit jeweils zugleich 75 % der finanziellen Beiträge reflektieren muss, macht das Prozedere nicht nur kompliziert, sondern vertieft auch das Übergewicht der Kommission bei Entscheidungen. Das nur schwache Stimmengewicht der Mitgliedstaaten dürfte der Akzeptanz von Entscheidungen abträglich sein.

Beachtenswert ist weiterhin, dass trotz des sehr breiten Ziel- und Aufgabenspektrums im Verordnungsentwurf lediglich eine grobe innere Struktur des Kompetenzzentrums festgelegt ist. Das einzige Entscheidungsorgan ist der Verwaltungsrat. Die Probleme und Themen im Bereich der Cybersicherheit und auch die Ausarbeitung des Finanzierungsplans sind aufwändig und erfordern spezifische Expertise. Diesen Aufgaben kann nur effektiv nachgekommen werden, wenn zur Entlastung des Verwaltungsrats weniger gewichtige Einzelfragen und solche des täglichen Geschäfts delegiert werden können. Allerdings fehlen hierfür geeignete Substrukturen. Deren Schaffung im weiteren Verlauf des Gesetzgebungsprozesses wäre ratsam, um eine sinnvolle und effiziente Aufgabenverteilung innerhalb des Kompetenzzentrums sicherzustellen.

Der Verordnungsentwurf enthält außerdem keine Angaben zur Ausgestaltung des Entscheidungsprozesses im Verwaltungsrat, also dazu, wie Informationen gesammelt und Entscheidungen vorbereitet werden, ob und wie ausführlich Entscheidungen zu begründen sind oder wie mit Interessenkonflikten umzugehen ist. Zwar besteht ein Recht des Verwaltungsrats, sich Regeln zur Vorbeugung, Vermeidung und den Umgang mit Interessenkonflikten zu setzen (Art. 42), jedoch keine Pflicht. Ein solcher Mangel an prozeduralen Bindungen führt zu einem weiten Ermessensspielraum mit wenig Kontrollmöglichkeiten. Die daraus resultierende Intransparenz ist unter rechtsstaatlichen Gesichtspunkten nicht wünschenswert.[20] Ein europäischer prozedural-administrativer Standard in Form eines europäischen Verwaltungsver-

fahrensrechts fehlt leider nach wie vor, wenngleich es dafür durchaus Vorschläge gibt.[21]

Wenig gelungen ist auch die Ausgestaltung des wissenschaftlich-technischen Beirats. Die Einbindung von Interessenvertretern in das Kompetenzzentrum erfolgt ohne echten Einfluss auf die Entscheidungsprozesse. Der Beirat kann keine verbindlichen Empfehlungen abgeben und es besteht keine Verpflichtung des Exekutivdirektors und des Verwaltungsrats, den Beirat wenigstens zu konsultieren. Wertvolles Wissen um die Standpunkte der Interessenvertreter und ihre Expertise auf dem Gebiet der Cybersicherheit bleiben auf diese Weise ungenutzt.

Einer der wesentlichen Streitpunkte im noch andauernden Gesetzgebungsprozess ist schließlich die Finanzierung des Kompetenzzentrums. Die vorgesehene Aufteilung der Kosten zwischen der Union und den Mitgliedstaaten bedeutet für Letztere, dass sie einen doppelten Beitrag zu leisten hätten: Jeder Mitgliedstaat leistet ohnehin Beiträge an die EU, aus denen diese „ihre" Finanzmittel zum Kompetenzzentrum beisteuert. Hinzukommen würden nun direkte Beiträge zum Kompetenzzentrum. Entsprechend gering ist die Akzeptanz des vorgeschlagenen Finanzierungsmodus seitens der Mitgliedstaaten. Der Rat hat deswegen vorgeschlagen, dass die EU die operativen und administrativen Kosten allein tragen soll[22] während den Mitgliedstaaten die Möglichkeit freiwilliger (finanzieller)

Beiträge für gemeinsame Aktivitäten eingeräumt würde.[23]

cc) Verhältnis zu ENISA

Das Kompetenzzentrum wäre neben der Agentur für Netz- und Informationssicherheit (ENISA)[24] eine zusätzliche europäische Einheit auf dem Gebiet der Cybersicherheit. Im Verordnungsentwurf finden sich allerdings nur wenige und eher allgemein gehaltene Hinweise dazu, in welchem Verhältnis beide zueinanderstehen sollen.[25] Insgesamt wird der ENISA eine eher untergeordnete Position eingeräumt, was in doppelter Hinsicht überraschend ist. Zum einen nimmt die Agentur eine hervorgehobene Position in der NIS-Richtlinie ein, wo sie ein vollwertiges Mitglied der Kooperationsgruppe ist und ihr wesentliche Unterstützungsaufgaben zukommen.[26] Zum anderen ergeben sich aus der ENISA-Verordnung verschiedene Aufgaben der Agentur, die sich mit den Aktivitäten des Kompetenzzentrums überschneiden.[27] Es wäre daher sinnvoll, das Verhältnis des Kompetenzzentrums zur ENISA im Verordnungsvorschlag detaillierter zu adressieren, nicht zuletzt um dem Eindruck zu begegnen, dass hier zwei Institutionen zueinander in Konkurrenz gestellt werden. Das wäre nämlich schon im Hinblick auf die Verteilung der knappen finanziellen Ressourcen kritikwürdig. Ohne eine klare Abgrenzung werden sich außerdem die vorhandenen Kapazitäten nicht effektiv nutzen lassen, weil notwendige Anstrengungen doppelt, gar nicht oder schlimmstenfalls widersprüchlich ausgeführt werden. Das Verhältnis zwischen Kompetenzzentrum und ENISA hat inzwischen jedoch Eingang in die Agenda des Europäischen Parlaments und des Rats gefunden,[28] so dass auf eine Klärung zu hoffen ist.

b) Nationale Zentren

Es soll zudem ein europaweites Netzwerk nationaler Koordinierungszentren entstehen.

aa) Aufgaben, Struktur und Finanzierung

Hierfür ist jeder Mitgliedstaat verpflichtet, ein nationales Koordinierungszentrum zu benennen, das die in der Verordnung vorgesehenen Aufgaben wahrnimmt (Art. 7 I). Die Kommission überprüft die Befähigung der Institution gem. Art. 6 IV im Rahmen einer Akkreditierung. Das Zentrum muss dabei über technisches Fachwissen im Bereich der Cybersicherheit verfügen oder direkten Zugang dazu haben und befähigt sein, sich wirksam mit der Industrie, dem öffentlichen Sektor und der Forschungsgemeinschaft auszutauschen und zu koordinieren (Art. 6 IV). Die einzelnen nationalen Koordinierungszentren bilden zusammen mit dem Kompetenzzentrum ein europaweites Netz, dessen Beziehungen und Aufgabenverteilung durch bilaterale Verträge der nationalen Zentren mit dem Kompetenzzentrum geregelt werden (Art. 6 V, VI). Für die nationalen Zentren ist keine paritätische Finanzierung vorgesehen. Art. 7 III erwähnt lediglich, dass die Union Finanzhilfen gewähren kann, was im Übrigen eine Finanzierung durch die Mitgliedstaaten voraussetzt. Aufgaben der nationalen Zentren sind gem. Art. 7 I die Unterstützung des Kompetenzzentrums in dessen Zielen und bei der Koordinierung der Kompetenzgemeinschaft, die Prüfung der Anträge auf Aufnahme in diese Gemeinschaft, die Erleichterung der Teilnahme an grenzüberschreitenden Projekten für Akteure aus den Mitgliedstaaten, das Wirken als nationale Kontaktstelle und die Schaffung von Synergien bei Aktivitäten auf nationaler und regionaler Ebene. Sie sollen ferner einen Beitrag zur Identifikation und Lösung von sektorspezifischen Cybersicherheitsproblemen leisten, Projekte des Kompetenzzentrums durchführen und die Arbeiten des Netzes, des Kompetenzzentrums und der Kompetenzgemeinschaft auf nationaler und regionaler Ebene fördern und verbreiten.

bb) Kritik

Der Verordnungsentwurf enthält keine Regelungen, wie die nationalen Koordinierungszentren untereinander zusammenarbeiten sollen. Davon auszugehen, dass die Mitgliedstaaten bzw. Koordinierungszentren selbst regeln werden, ob und wie sie miteinander interagieren, ist bestenfalls optimistisch. Eher ist anzunehmen, dass die Mitgliedstaaten weiterhin nationale Strategien verfolgen oder lediglich bereits bestehende Interaktionen fortgesetzt werden. Auf diese Weise entsteht kein echtes Netzwerk und bleibt unter Umständen wertvolles Potenzial ungenutzt.

Abzuwarten bleibt, ob es eine Verpflichtung der Mitgliedstaaten geben wird, nur öffentliche Institutionen als nationale Koordinierungszentren zu benennen. Der Rat hat sich deutlich hierfür ausgesprochen.[29] Die darin zum Ausdruck kommende Haltung ist insofern wenig überraschend, als die nationalen Koordinierungszentren eine wichtige Rolle bei der Verteilung der Finanzmittel[30] einnehmen sollen.

c) Kompetenzgemeinschaft für Cybersicherheit

Als dritte Einrichtung sieht der Entwurf die Institutionalisierung der Kompetenzgemeinschaft für Cybersicherheit vor.

aa) Aufgaben, Struktur und Finanzierung

Die Kompetenzgemeinschaft soll die wichtigsten Interessenvertreter im Bereich der Cybersicherheit zusammenbringen (Art. 8 II). Das

Kompetenzzentrum akkreditiert Einrichtungen als Mitglieder der Kompetenzgemeinschaft, nachdem das jeweilige nationale Koordinierungszentrum das Vorliegen der Aufnahmevoraussetzungen (Art. 8 III) geprüft hat (Art. 8 IV). Auch Stellen, Ämter und Agenturen können für die Gemeinschaft akkreditiert werden (Art. 8 V).

Die Kompetenzgemeinschaft unterstützt das Kompetenzzentrum in der Erfüllung seines gesetzlichen Auftrags und seiner Ziele und fördert und verbreitet das Fachwissen zu Cybersicherheit in der EU (Art. 8 I, 9 Nr. 1), beteiligt sich an von den Zentren geförderten Tätigkeiten, an im Arbeitsplan des Kompetenzzentrums vorgesehenen Maßnahmen sowie den von seinem Verwaltungsrat eingesetzten Arbeitsgruppen (Art. 9 Nr. 2, 3). Die Mitglieder unterstützen die Zentren bei der Förderung von Projekten. Außerdem unterstützen und verbreiten sie die Ergebnisse der von ihnen durchgeführten Tätigkeiten und Projekte (Art. 9 Nr. 4, 5). Die Finanzierung dieser Aufgaben ist noch nicht gesetzlich geklärt.

bb) Kritik

Obwohl die Aufgaben der Kompetenzgemeinschaft vielfältig klingen, ist ihre tatsächliche Einbindung in das Netzwerk nicht klar und unzureichend geregelt. Wie bereits am Beispiel des wissenschaftlich-technischen Beirats kritisiert, fehlt eine geeignete Struktur, die der Kompetenzgemeinschaft eine proaktive Einbringung ermöglichen würde. Stattdessen wird die Einbeziehung ausschließlich „von oben nach unten" gedacht, ausgehend vom europäischen Kompetenzzentrum oder von den natio-

nalen Koordinierungszentren zur Kompetenzgemeinschaft hin. Der umgekehrte Weg „von unten nach oben" ist nicht vorgesehen. Immerhin scheint es aber, dass ein diesbezüglicher Änderungsbedarf vom Europäischen Parlament erkannt wurde.[31]

Durch die Regelungen zur Akkreditierung, die die Entscheidungsmacht über die Relevanz eines Anwärters auf die mitgliedstaatliche und EU-Ebene konzentrieren, wird der Kompetenzgemeinschaft selbst trotz gerade dort vorhandener Expertise kein Mitspracherecht eingeräumt. Zudem ist nicht klar, ob die Initiative für eine Mitgliedschaft allein vom nationalen Koordinierungszentrum oder auch vom Anwärter selbst ausgehen kann. Wie in Anbetracht dieser Ausgestaltung und der offenen Fragen zur Finanzierung die notwendige Mobilisierung der Kompetenzgemeinschaft zu aktiver Mitwirkung an der Verbesserung europäischer Cybersicherheit gelingen soll, ist sehr fraglich.

IV. Sinnvolle Netzwerksteuerung im Lichte europäischer Werte

Eine Erhöhung europäischer Cybersicherheit trägt nicht nur zur Förderung des Binnenmarktes und der Unabhängigkeit der Union von Drittstaaten beim Schutz der Gesellschaft vor Cybergefahren bei. Vielmehr dient europäische Cybersicherheit auch der Stärkung der Union als sicherer Hafen für Menschenrechte und als Garant einer demokratischen und freiheitlichen Gesellschaft. Voraussetzung für den Erfolg des Cybersicherheitsnetzwerks ist jedoch eine sinnvolle Netzwerksteuerung.

Allgemein lassen sich hierarchische und heterarchische Steuerungsansätze mit jeweils spezifischen Vor- und Nachteilen unterscheiden. Rein hierarchische Ansätze eignen sich grundsätzlich für den Aufbau von Anordnungs- und Kontrollstrukturen mit schneller Reaktions- und verbindlicher Entscheidungsfähigkeit. Die Vorteile dieses Ansatzes finden ihre Grenzen jedoch in den zeitlichen Ressourcen und dem immer nur begrenzt vorhandenen Wissen der Entscheidungsträger.[32] Nimmt man andererseits rein heterarchische Steuerungsansätze in den Blick, fehlt solchen Netzwerken aufgrund der Gleichwertigkeit der Mitglieder die Fähigkeit, in wichtigen Fragen schnell verbindliche Entscheidungen zu treffen und die Etablierung von effektiven Kontrollmechanismen ist nur begrenzt möglich. Das Potenzial solcher Strukturen liegt vielmehr in ihrer Eignung als Sammelbecken für das breite Wissen und die Expertise von Industrie, Forschung und spezifischen Interessenträgern. Auf diese Weise lässt sich sehr leicht nicht nur die Wissensbeschaffung, sondern auch -verteilung organisieren.[33]

Eine Kombination der Ansätze ermöglicht, ihre jeweiligen Vor- und Nachteile auszugleichen und durch das konkrete Strukturdesign Synergieeffekte nutzbar zu machen. Es gilt als ein wesentliches Charakteristikum solcher Netzwerke, dass sich in ihnen besonders gut Wissen durch die Zusammenarbeit zwischen öffentlichen und privaten Akteuren sammeln lässt.[34] Je nach Anforderungsfeld kann so eine passgenaue Steuerungsstruktur für ein konkretes Netzwerk mit spezifischen Aufgaben geschaffen werden.

Ein kombinierter Steuerungsansatz für das europäische Cybersicherheitsnetzwerk sollte insofern nach der Art der zutreffenden Entscheidungen, zB strategische oder alltägliche administrative, unterscheiden und sie jeweils einer geeigneten Hierarchiestufe zuordnen. Dazu sollten innerhalb des Kompetenzzentrums Substrukturen eingeführt werden. Berücksichtigt werden muss auch die dynamische Entwicklung des Cybersicherheitsmarktes. Die Netzwerkstruktur sollte deswegen unbedingt das sich ebenfalls dynamisch entwickelnde Fachwissen von Akteuren der Industrie und Wissenschaft mit ihren Interessen aktiv einbeziehen. Das Konzept des technisch-wissenschaftlichen Beirates sollte insofern grundsätzlich überdacht werden. Es wäre sinnvoller, eine echte Interessenvertretung einzusetzen, die in sich eine breite Diversität aufweist und deren Empfehlungen vom Verwal-

tungsrat zu berücksichtigen bzw. Abweichungen hiervon zu begründen sind. Für die Kompetenzgemeinschaft in einer echten Netzwerkstruktur sollte auch die Möglichkeit geschaffen werden, sich ausgerichtet an aktuellen Problemen, Fragestellungen, Bedürfnissen und Entwicklungen selbst zu organisieren, den Austausch mit dem Kompetenzzentrum und den nationalen Koordinierungszentren zu koordinieren und so insgesamt die Fragmentierung im Bereich der Cybersicherheit zu reduzieren. Denkbar wäre zB die Einrichtung von Knotenpunkten der Kompetenzgemeinschaft, in denen gebündelt ein geschützter Wissensaustausch stattfinden, interdisziplinäre Problemlösungen erarbeitet und auch Finanzierungsmöglichkeiten für bestimmte Forschungs- und Entwicklungsprojekte erschlossen werden könnten.

V. Fazit

Der Europäische Rechnungshof identifizierte 2019 vier Gruppen von Herausforderungen für die zukünftige Cyberpolitik der EU: die Schaffung einheitlicher, angemessener politischer und rechtlicher Rahmenbedingungen, eine Verbesserung der Finanzierung, eine Stärkung der Resilienz und die Möglichkeit, wirksam auf Cybervorfälle zu antworten.[35] Andere sehen den intergouvernementalen Charakter der Union und das gleichzeitige Fehlen einer kollektiven Vision für Cybersicherheit zwischen der EU und den Mitgliedstaaten

als den limitierenden Faktor für die Rolle der Union als zentrale Spielerin in der weltweiten Cybersicherheit.[36] Und auch die fehlende Umsetzung der vorhandenen wissenschaftlichen Exzellenz im Bereich der Cybersicherheit in marktfähige Produkte wird als ein wesentliches Problem der EU benannt.[37]

Mit dem Verordnungsentwurf adressiert die EU diese zentralen Herausforderungen und Schwächen ihrer bisherigen Cybersicherheitspolitik und macht sie für die nächsten Jahre zu einem Betätigungsfeld von herausgehobener Bedeutung. Der Plan, Cybersicherheit durch Institutionalisierung zukunftsfest und als Wettbewerbsvorteil zu einer tragenden Säule des europäischen Binnenmarktes zu machen, stellt einen gelungenen und wichtigen Ansatz für die organisierte Cybersicherheitspolitik in Europa dar. Auch international wird er als erfolgreicher Versuch rezipiert, die internationale Führungsrolle auf dem Gebiet der Cybersicherheit anzustreben.[38]

Wie die vorhergehende Untersuchung gezeigt hat, besteht jedoch noch erheblicher Verbesserungsbedarf bezüglich des gewählten Steuerungsansatzes für das Netzwerk. Das Verhältnis der unterschiedlichen Akteure zueinander, die Zusammenarbeit in und zwischen den vorgesehenen Institutionen sowie die hierfür erforderlichen Entscheidungsprozesse erfahren bisher eine zu rudimentäre gesetzliche Ausgestaltung, um in der europäischen Praxis erfolgversprechend funktionieren zu können. Es darf, wie ebenfalls gezeigt, jedoch darauf gehofft werden, dass diese problematischen Punkte im weiteren Gesetzgebungsverfahren adressiert und ausgeräumt werden.

* Professorin *Dr. Spiecker gen. Döhmann* ist Inhaberin des Lehrstuhls für Öffentliches Recht, Informationsrecht, Umweltrecht, Verwaltungswissenschaften an der Goethe-Universität Frankfurt a. M., an dem die beiden weiteren Autoren als Wissenschaftliche Mitarbeiter tätig sind. Der Lehrstuhl beteiligt sich am Pilotprojekt CyberSec4Europe (Forschungsprojekt im Rahmen des EU-Förderungsprogramms „Horizon 2020"), dessen Leitung und Koordination

bei der Goethe-Universität Frankfurt a. M. liegen. – Der Beitrag basiert auf einem Vortrag für die Herbstakademie der Deutschen Stiftung für Recht und Informatik.

1 Kontext des Vorschlags VO (EU) 2018/0328 (COD).
2 Erwägungsgrund 6 Vorschlag VO (EU) 2018/0328 (COD).
3 Erwägungsgrund 6 Vorschlag VO (EU) 2018/0328 (COD).
4 Erwägungsgrund 6 Vorschlag VO (EU) 2018/0328 (COD).
5 *Richter/Spiecker gen. Döhmann* in *Durner* ua, Gedächtnisschrift Arndt Schmehl, 2019, 181 f. mwN.
6 Art. 2, 10 I EUV.
7 Präambel, Art. 2 EUV.
8 *Hofmann* in *Barnard/Peers*, European Union Law, 2. Aufl. 2017, 208.
9 *Augsberg* in *Terhechte*, Verwaltungsrecht der Europäischen Union, 2012, § 6 Rn. 38.
10 *Calliess* in *Calliess/Ruffert*, EUV/AEUV, 5. Aufl. 2016, EUV Art. 13 Rn. 31; *Streinz* in *Streinz*, EUV/AEUV, 3. Aufl. 2018, EUV Art. 13 Rn. 32, 34.
11 *Calliess* in *Calliess/Ruffert*, EUV Art. 5 Rn. 6 ff.; *Pache* in *Pechstein/Nowak/Häde*, Frankfurter Kommentar zu EUV, GRCh, AEUV, Bd. 1 EUV und GRCh, 2017, EUV Art. 5 Rn. 22; *Streinz* in *Streinz*, EUV Art. 5 Rn. 8 f.
12 Vorschlag für eine VO über das Rahmenprogramm für Forschung und Innovation „Horizont Europa", COM(2018), 435.
13 Vorschlag VO (EU) 2018/0328 (COD), 3.
14 Vorschlag VO (EU) 2018/0328 (COD), 1 ff.
15 Vorschlag für eine VO zur Aufstellung des Programms „Digitales Europa" für den Zeitraum 2021–2027, COM(2018), 434.
16 Vorschlag VO (EU) Nr. 2018/0328 (COD), 3.
17 EESC 2018/05208, OJ C 110, 22.3.2019, 72–74; EESC 2018/04805, OJ C 159, 10.5.2019, 63–67.
18 AD/2019/630409, 31.1.2019, https://www.europarl.europa.eu/RegData/commissions/imco/avis/2019/630409/IMCO_AD(2019)630409_DE.pdf (12.6.2020).
19 CyberSec4Europe D2.1 Governance Structure, Figure 1, https://cybersec4europe.eu/wp-content/uploads/2020/02/D2.1-Governance-Structure-final-Submitted.pdf (17.9.2020).
20 *Hofmann* in *Barnard/Peers*, 209 f.
21 *Schneider* ua, ReNEUAL – Musterentwurf für ein EU-Verwaltungsverfahrensrecht, 2015.
22 Vorschläge und Anmerkungen 368 und 389, Interinstitutionelles Dossier 2018/0328 (COD) Dok. Nr. 7616/19 v. 26.3.2019, https://data.consilium.europa.eu/doc/document/ST-7616-2019-INIT/en/pdf (12.6.2020).
23 Vorschläge und Anmerkungen 1982, 265 und 376, Interinstitutionelles Dossier 2018/0328 (COD) Dok. Nr. 7616/19 v. 26.3.2019.
24 VO (EU) 2019/881 des Europäischen Parlaments und des Rates v. 17.4.2019 – ABlEU L 151 v. 7.6.2019, 15 ff.
25 Erwägungsgrund 21, Art. 4 V a), 12 VII Vorschlag VO (EU) Nr. 2018/0328 (COD).
26 Art. 11 II, III RL 2016/1148/EU.
27 Art. 4, 6, 7, 9, 11 VO (EU) 2019/881.
28 Standpunkt des Europäischen Parlaments in erster Lesung P8_TA (2019)0419; Vorschläge und Anmerkungen Interinstitutionelles Dossier 2018/0328 (COD), Dok. Nr. 7616/19 v. 26.3.2019.
29 Vorschlag und Anmerkung 27 Interinstitutionelles Dossier 2018/0328 (COD), Dok. Nr. 7616/19 v. 26.3.2019.
30 Art. 7 I f) Vorschlag VO (EU) 2018/0328 (COD).
31 Abänd. 111, 119 iVm 83, 124, 151 P8_TA (2019)0419.
32 Siehe Nr. 3.2.1.2.
33 *Mayntz* in *Benz/Dose*, Governance – Regieren in komplexen Regelsystemen, 2. Aufl. 2010, 73.
34 *Schwind*, Netzwerke im Europäischen Verwaltungsrecht, 2017, 131 f.
35 Europäischer Rechnungshof, Herausforderungen für eine wirksame Cybersicherheitspolitik der EU, 4.
36 *Sliwinski*, Contemporary Security Policy (35) 2014, 468.
37 Vorschlag VO (EU) 2018/0328 (COD), 2.
38 *Westby*, Why the EU is about to seize the global lead on cybersecurity, 31.10.2019, https://www.forbes.com/sites/jodywestby/2019/10/31/why-the-eu-is-about-to-seize-the-global-lead-on-cybersecurity/#4df878252938 (12.6.2020).