Bayerisches Staatsministerium des
Innern, für Sport und Integration

Rede des Bayerischen Staatsministers des
Innern, für Sport und Integration, Joachim Herrmann,

anlässlich der Fachtagung
„Going dark – Signals Intelligence im IT-Zeitalter“

am Montag, 4. Oktober 2021 in München

Es gilt das gesprochene Wort!

Begrüßung

Dozentinnen und **Dozenten**,

Damen und **Herren**,

auch ich darf Sie recht herzlich zu unserer Fachtagung in der Alten Kongresshalle in München **begrüßen**.

Anschläge von Würzburg und Ansbach

Der islamistische **Attentäter von Würzburg**, der **im Juli 2016** in einem Regionalzug **mehrere Menschen mit einer Axt** schwer **verletzte**, wurde **sogar noch während der Tatausführung** von **IS-Hintermännern** im Nahen Osten **über verschlüsselte Messengernachrichten** „**ferngesteuert**“. Ebenso der **Ansbacher Attentäter**, der wenige Tage später mit einem **Sprengsatz** sich selbst tötete und dabei 15 Menschen verletzte.

Amri-Anschlag Breitscheidplatz Berlin

Auch **Anis Amri** schickte bei seinem schrecklichen **Anschlag im Dezember 2016** auf dem **Berliner Breitscheidplatz noch während der Fahrt** mit dem gestohlenen Lkw über Telegram **Nachrichten an Dritte**.

Das alles zeigt die **große Bedeutung**, die **modernen Kommunikationsmitteln** heutzutage auch bei Attentaten zukommt.

Frage nach dem „Warum“

Wenn solche verabscheuungswürdigen und verheerenden Taten geschehen, stellen sich unsere Bürgerinnen und Bürger zu Recht die **Frage**: Hätten die **Sicherheitsbehörden** das nicht **verhindern** können? In **Gerichtsverfahren**, **Parlamentarischen Untersuchungsausschüssen und wissenschaftlichen Gutachten** werden die Fälle mit enormem Aufwand **untersucht**. Und ja, es finden sich dann mitunter auch Hinweise, dass Informationen bisweilen nicht berücksichtigt, falsch eingeordnet oder nicht rechtzeitig weitergegeben wurden.

Strukturelles Problem: Fortschritt der IT-Technik

Wer aber die Frage nach dem „Warum“ **allein** mit **behördlichen und damit menschlichen Fehlern** beantworten will, verschließt die Augen davor, dass wir es hier **zugleich mit strukturellen Problemen grundsätzlicher Art** zu tun haben.

Sie ergeben sich aus den enormen **Fortschritten der Informationstechnik** und nehmen dabei **völlig neue Dimensionen** an.

EncroChat

Drastisch vor Augen geführt hat uns das im vergangenen Jahr der **Fall EncroChat**, einem **Instant-Messengerdienst**, der ein **verschlüsseltes Kommunikationsnetz mit speziellen Kryptohandys** anbot. Nachdem es im Rahmen von Ermittlungen **französischen und niederländischen Behörden gelungen** war, sich **Zugriff auf einen Server** von EncroChat zu verschaffen, bestätigte sich ein schrecklicher Verdacht: Das Netzwerk wurde **fast ausschließlich von der Organisierten Kriminalität** genutzt – **allein im zweiten Quartal 2020** konnten die Behörden mehr als **100 Millionen Nachrichten mitlesen**.

Vor den Augen der Ermittler öffnete sich das **Tor zu einer Welt voller Abgründe**, in der **Brutalität** und **Grausamkeit** an der Tagesordnung stehen. Nach Mitteilung des **Bundeskriminalamts** wurden allein in

Deutschland bislang **mehr als 2.250 Ermittlungsverfahren eingeleitet**, mehr als **750 Haftbefehle** vollstreckt und **mehrere Tonnen an Drogen sichergestellt**. Viele der Verdächtigten verfügten über **Waffen**, **teilweise** sogar **verbotene Kriegswaffen**.

Verbreitung von Verschlüsselungstechnik

Meine **Damen** und **Herren**, dieses Beispiel zeigt sehr deutlich: Die **Verbreitung von Verschlüsselungstechnik** ist **nicht nur ein Gewinn für die Privatsphäre**, sondern auch eine **enorme Herausforderung für die Sicherheitsbehörden**. Denn bereits die **standardmäßige Ende-zu-Ende-Verschlüsselung** in überaus verbreiteten Messengerdiensten wie WhatsApp weist einen derart **hohen Verschlüsselungsgrad** der Chats auf, dass der Inhalt **grundsätzlich nicht von Dritten mitverfolgt** werden kann.

Auch die **Inhalte von Internetportalen**, **Festplatten**, **Smartphones oder Cloudspeichern** können durch **kostenlose Open-Source-Programme** und Standardeinstellungen durch **jedermann** vor **Zugriff**

Dritter geschützt werden. Solche Verschlüsselungen mit der „**Holzhammer-Methode**“ zu **knacken**, indem man durch Rechenroutinen **systematisch alle denkbaren Schlüssel oder Passwörter ausprobiert**, erfordert **enorme Rechenkapazitäten** und funktioniert unter Umständen auch **nur bei schwachen Passwörtern**.

5G-Standard

Im Bereich der **Mobilfunktechnik** sorgt zudem der **5G-Standard** generell dafür, dass die Kennung, die der eindeutigen Identifizierung der Netzteilnehmer dient, **nur noch verschlüsselt** übermittelt wird.

Fortschritte der Quantentechnologie

Die immer weiter voranschreitende technische Entwicklung, insbesondere im Bereich der **Quantentechnologie**, wird uns künftig außerdem noch vor weitere **sicherheitsrelevante Herausforderungen** stellen.

„Going dark“ rüttelt an Grundfesten des Staates

Der Inhalt einer digitalen, kryptierten **Kommunikation von Terroristen**, **Extremisten und Kriminellen kann grundsätzlich**

nicht mehr von den Sicherheitsbehörden mitverfolgt werden. Darin liegt nicht nur irgendeines unter vielen technischen Problemen bei der Ermittlungsarbeit. Das „**Going dark**“**-Phänomen** rüttelt damit an den **Grundfesten des Staates**, weil er die **Sicherheit seiner Bürgerinnen und Bürger so nicht mehr garantieren** kann.

Handlungsinstrumente der Sicherheitsbehörden

Den **Staat** trifft **auch und gerade in einer digitalisierten Welt** die **Verpflichtung**, **unsere Freiheit und unsere Rechtsordnung zu verteidigen**. Die **gesetzlichen Handlungsinstrumente**, die den **Sicherheitsbehörden** hierfür derzeit zur Verfügung stehen, sind **leider eher überschaubar**.

Quellen-TKÜ

In **Bayern** haben wir etwa die **Polizei und das Landesamt für Verfassungsschutz** mit der **Befugnis** zur **Quellen-Telekommunikationsüberwachung** ausgestattet. So darf **Telekommunikation** – unter bestimmten **gesetzlichen Voraussetzungen** und nach Prüfung durch einen

Richter beziehungsweise die **G 10-Kommission** – **überwacht** und aufgezeichnet werden, **bevor** eine **Verschlüsselung** oder **nachdem** die **Entschlüsselung** erfolgt.

Online-Durchsuchung

Polizei und Verfassungsschutz verfügen in Bayern auch über die **Befugnis**, **verdeckt auf informationstechnische Systeme zuzugreifen** – die sogenannte **Online-Durchsuchung** beziehungsweise **Online-Datenerhebung**. Auch auf diesem Weg können unter Umständen **Informationen erlangt** werden, die **zunächst verschlüsselt übertragen**, anschließend aber **unverschlüsselt auf einem Endgerät abgespeichert** wurden.

Widerstand der SPD gegen Online-Durchsuchung für BfV

Auf Bundesebene musste allerdings die zunächst **vom Bundesinnenministerium für das Bundesamt für Verfassungsschutz vorgesehene Befugnis** zur Online-Datenerhebung wegen des **Widerstands der SPD** gestrichen werden. Und das **obwohl** eine entsprechende Befugnis den **Strafverfolgungsbehörden bereits**

zur Verfügung steht. Der **am Ende der Legislaturperiode verabschiedete Minimalkompromiss** beinhaltet **lediglich** eine **Befugnis der Verfassungsschutzbehörden von Bund und Ländern zum Einsatz der Quellen-TKÜ**.

Verkehrsdatenspeicherung

Auch der **Zugriff auf die von Telekommunikationsunternehmen gespeicherten Verkehrsdaten** würde den Sicherheitsbehörden helfen, ihre schwindenden Möglichkeiten zu **kompensieren**, die Inhalte der Telekommunikation zu erfassen – von Kritikern im öffentlichen Diskurs mit der **irreführenden Bezeichnung** als „**Vorratsdatenspeicherung**“ **diskreditiert**. Denn **Informationen darüber**, **wer wann mit wem von wo und mit welchem Gerät telefoniert** hat, bieten häufig auch **unabhängig vom Inhalt** der Kommunikation **wichtige Ermittlungsansätze**.

Derzeit hat die **Bundesnetzagentur** allerdings die **gesetzliche Speicherpflicht** der

Telekommunikationsanbieter **faktisch ausgesetzt**, weil die deutschen Regelungen derzeit dem **Europäischen Gerichtshof vorliegen**.

„Going dark“

Meine **Damen** und **Herren**, ich glaube **nicht**, dass wir **mit den bestehenden Befugnissen langfristig** ein „**Going dark**“ **vermeiden** können! Wir müssen daher vor dem Hintergrund des **rasanten technologischen Fortschritts dringend** die **Effektivität** der derzeit bestehenden Handlungsmöglichkeiten **fortlaufend kritisch beleuchten**.

Was **in der analogen Welt selbstverständlich** war, kann **in einer digital vernetzten Welt nicht ersatzlos wegfallen**! Schon seit den **Anfangsjahren der Bundesrepublik Deutschland** war es den Sicherheitsbehörden **gestattet**, bei Vorliegen der gesetzlichen Voraussetzungen aufgrund einer richterlichen Entscheidung **Briefe zu öffnen und Telefonate mitzuhören** – beides war in praktischer Hinsicht ohne größere Hindernisse umsetzbar.

Verschlüsselte Nachrichten sind die verschlossenen Briefe des 21. Jahrhunderts. Die **Herausforderungen** sind jedoch inzwischen **so groß**, dass die **bestehenden Überwachungsbefugnisse in weiten Teilen schlichtweg ins Leere laufen**. Das liegt **nicht nur am technischen Fortschritt**, sondern auch an den **hohen verfassungsrechtlichen Hürden**, die das **Bundesverfassungsgericht** für den Einsatz moderner Überwachungstechniken **vorschreibt**. Dazu werden wir von Ihnen, **lieber Herr Professor Kirchhof**, **noch Näheres** hören.

Verschlüsselung als Eckpfeiler der Cybersicherheit

Selbstverständlich stellt die Verschlüsselung aber auch einen **wesentlichen Eckpfeiler der Cybersicherheit** dar. Denn ein **Verzicht auf Verschlüsselung** kann genauso wie eine **defizitäre Technik neue Gefahren für die Sicherheit** befördern. Beispielsweise wurden Anfang des Jahres die **Daten von mehr als 533 Millionen Facebook-Nutzern** im Internet **veröffentlicht**, die Hacker 2019 abgegriffen hatten.

Schäden für die Wirtschaft

Cyberspionage verursacht **jährlich Schäden in Milliardenhöhe**, kostet wertvolle **Arbeitsplätze** und entzieht unserem Land bedeutende **Wettbewerbsvorteile**.

Notwendigkeit effektiven Schutzes

Gerade **für Unternehmen** ist es daher **essentiell**, die **Daten ihrer Kunden sowie Betriebs- und Geschäftsgeheimnisse effektiv vor Diebstahl und Spionage zu schützen**. Gleiches gilt natürlich für **Behörden**.

„Internet of things“ KRITIS

Ferner erfordert **die umfassende Vernetzung im „Internet of things“** eine **Absicherung gegen Sabotage**. **Kritische Infrastrukturen** können leicht zum Ziel von **Hacker-Gruppen** werden, wie sie leider auch **von manchen ausländischen Staaten offensiv eingesetzt** werden.

Grundsatz „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“

Was können wir also tun, um **Licht ins Dunkel zu bringen**, **ohne dunklen Kräften an anderer Stelle Vorschub zu leisten**? Die von der **Bundesregierung** zum Ende der letzten Legislaturperiode beschlossene „**Cybersicherheitsstrategie**

2021“ verfolgt hier **im Einklang mit** dem **Rat der Europäischen Union** den **Grundsatz** „**Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung**“.

Förderung von Verschlüsselungstechnik

Privatsphäre und **Sicherheit der Kommunikation** gilt es durch Verschlüsselung zu **schützen**. **Gleichzeitig** muss aber für die zuständigen **Behörden** auch in der digitalen Welt die Möglichkeit bestehen, über einen **rechtmäßigen Zugang zu Daten für legitime und klar definierte Zwecke** im Rahmen der **Bekämpfung schwerer Kriminalität wie Kinderpornographie und Terrorismus** zu verfügen und die **Rechtsstaatlichkeit** so zu **wahren**.

Das kommt einer „**Quadratur des Kreises**“ gleich. Ich sehe hier daher **alle drei Gewalten gefordert**: **Exekutive**, **Legislative und Judikative**.

Exekutive

Die **Exekutive** muss **Werkzeuge und Methoden entwickeln**, die den hohen **verfassungsgerichtlichen Anforderungen genügen**. Das ist bei den **auf dem Markt** verfügbaren **Instrumenten**, die **meist aus dem außereuropäischen Ausland** stammen, in der Regel **nicht gerecht**. Die 2017 errichtete **Zentrale Stelle für Informationstechnik im Sicherheitsbereich** *(ZITiS)* bildet daher meines Erachtens einen **Meilenstein** für die **Digitale Souveränität der deutschen Sicherheitsarchitektur**. ZITiS gilt es zu **stärken** und **weiter auszubauen**, auch unter Berücksichtigung der **länderspezifischen Interessen**.

Legislative

Dort, wo die **höchstrichterliche Rechtsprechung dem Gesetzgeber Möglichkeiten aufgezeigt und Gestaltungsspielräume belassen** hat, gilt es davon auch **konsequent Gebrauch** zu machen. Ich denke hier besonders an die **Nachrichtendienste**. Schon seit Langem fordere ich, dass dem **Bundesamt für Verfassungs-**

schutz die Befugnis zur **Online-Durchsuchung** eingeräumt und der Zugriff auf **gespeicherte Verkehrsdaten** eröffnet wird.

Judikative

Schließlich sehe ich auch die **Rechtsprechung in der Pflicht**, ihre **Vorgaben fortlaufend** vor dem Hintergrund der **rasanten technischen Entwicklung** und der daraus entstehenden **neuen Gefahren zu überprüfen**. **Mich** erfüllt es immer wieder mit **Staunen**, welche **Fülle an Detailvorgaben für den Gesetzgeber** das Bundesverfassungsgericht im Bereich des Sicherheitsrechts **aus dem Grundgesetz zu lesen** vermag.

Verhältnismäßigkeit als relative Grenze

Fast alle dieser Vorgaben **beruhen** auf Erwägungen der **Verhältnismäßigkeit im engeren Sinn**, ein **relativer Begriff**. **Je größer die Gefahr** auf der einen Seite der **Waagschale**, **desto mehr** darf der Gesetzgeber die Sicherheitsbehörden auch mit **Befugnissen zu deren Abwehr** ausstatten. Wir müssen stets aufs Neue abwägen.

Keine strategische Fernmeldeaufklärung im Inland?

Das gilt beispielsweise für die **apodiktische Aussage**, dass *„den Sicherheitsbehörden ein so weitreichendes Instrument wie die **anlasslose Telekommunikationsüberwachung innerstaatlich von vornherein nicht zur Verfügung gestellt** werden darf*“. Ich spreche von der sogenannten **strategischen Fernmeldeaufklärung**, wie sie der **Bundesnachrichtendienst in Bezug auf das Ausland** einsetzt.

Mir **leuchtet nicht** ein, warum es **ausnahmslos unverhältnismäßig** sein soll, an den **Knotenpunkten des Internets** anhand von **mehrstufigen Filter- und Suchfunktionen** nach Anhaltspunkten für **schwerste Bedrohungen existenzieller Rechtsgüter**, etwa **groß angelegte terroristische Anschläge**, zu suchen – zumal bei einer strengen Kontrolle in richterlicher Unabhängigkeit. Die **Belastung für den Einzelnen** ist doch **in beiden Fällen gering**, weil er **zunächst anonym in der Datenflut** bleibt – individuelle **Folgemaßnahmen** bedürfen erst einer **eigenen**

Anordnung auf der Grundlage der dafür erforderlichen **gesetzlichen Voraussetzungen**.

Schlussworte: Recht auf Sicherheit in der digitalisierten Welt

Ich will **nicht in Abrede stellen**, dass man das **auch anders sehen** kann. Vermutlich werden Sie, **lieber Herr Professor Kirchhof**, mir sogleich **widersprechen**. Bei allem **Diskussionsbedarf** ist und bleibt es aber **meine feste Überzeugung**: Die Bürgerinnen und Bürger dieses Landes haben **auch in der digitalisierten Welt ein Recht auf Sicherheit**! Wir müssen uns diesen **Herausforderungen der modernen Informationstechnik stellen** und im **Spannungsfeld zwischen individuellem Eingriffsschutz und staatlicher Schutzpflicht gemeinsam** nach **Lösungen suchen**.

Ich bin sicher: Diese **Fachtagung wird den Diskussionsprozess beleben**! Ich **freue** mich auf **anregende Beiträge** und den Austausch mit Ihnen.