Abgeordnete Eva-Maria Himmelbauer, BSc (ÖVP): Herr Präsident! Herr Bundesminister! Ich möchte zum Themenbereich Internetkriminalität kommen. Internetkriminalität im engeren Sinne ist vor allem illegaler Zugriff auf Computersysteme, Datendiebstahl, Datenbeschädigung, aber auch DDoS-Attacken, die Computersysteme einfach lahmlegen oder sabotieren. Im weiteren Sinne reden wir aber über alle Straftaten, Delikte, die mit dem Internet verbunden sind, beispielsweise Betrug, Erpressung et cetera.

Gerade im Bereich der Internetkriminalität sehen wir, dass im Jahr 2018 die Zahl der Straftaten, die bei rund 20 000 gelegen ist, eine massive Steigerung gegenüber dem Jahr 2017 aufwies. Ich möchte in meiner Fragestellung trotzdem vor allem zu dem engen Themenbereich Cybercrime kommen, weil dieser natürlich auch mit vielen Fragen verbunden ist:

120/M

„Welche Maßnahmen setzt die Bundesregierung, um die Bekämpfung von Cyber Crime weiter zu intensivieren?“

Präsident Mag. Wolfgang Sobotka: Bitte, Herr Bundesminister.

Bundesminister für Inneres Herbert Kickl: Danke, Frau Abgeordnete. Das ist wirklich ein Problembereich, dem man sich offen stellen muss und der selbstverständlich auch den Einsatz von neuen Ressourcen, sei es jetzt quasi Humankapital oder auch technisches Equipment, braucht, um das gute Niveau, das wir in anderen Bereichen haben, nämlich bei der Kriminalitätsbekämpfung im klassischen Sinn, halten zu können.

Wir haben vorher schon bei einem anderen Bereich darüber gesprochen, wie wichtig die Präventionskomponente ist. Wollen wir bei dieser Pyramide ganz unten beginnen, dann würde ich sagen, dass es für uns sehr, sehr wichtig ist, beginnend bei den Kindern, über die Einbindung in Projekten wie Gemeinsam Sicher, etwa mit den Wirtschaftstreibenden, ganz elementare Dinge die Cybersicherheit betreffend zu forcieren.

Das beginnt mit ganz einfachen Dingen, E-Mail-Sicherheit ist eine solche Komponente, Passwortsicherheit ist eine solche Komponente, das Herunterladen von neuen Versionen von Schutzprogrammen, und, und, und. Allein wenn es uns gelingt, da bewusstseinsbildend tätig zu sein, schließen wir ein ganz, ganz großes Einfallstor für Kriminelle im digitalen Bereich.

Wenn ich an der anderen Spitze ansetze, dann haben wir im Bundeskriminalamt auch eine entsprechende Hightecheinheit, das Cybercrime Competence Center, wirklich eine Elitetruppe, möchte ich einmal sagen, wenn es um den Bereich dieser Kriminalitätsbekämpfung geht. Als ich ins Amt gekommen bin, waren dort in etwa 50 Personen beschäftigt, jetzt sind es fast 70. Das heißt, wir bauen da kontinuierlich die Kapazitäten aus, und das stellt auch einen Schwerpunkt beim Einsatz unserer Personalressourcen dar.

Was wird im Bundeskriminalamt inhaltlich gemacht? – Da gibt es drei wesentliche Komponenten, wo man inhaltlich, glaube ich, sehr, sehr erfolgreich und konsequent arbeitet. Das eine ist der gesamte Bereich der Kryptowährungen, wo wir wissen, dass das eine immer größere Rolle im Bereich der organisierten Kriminalität spielt. Da haben wir sehr viel Kompetenz, wenn es um die Verfolgung dieser Zahlungsströme geht, wenn es um das Festmachen dieser Gelder geht, durchaus auch im Zusammenhang mit anderen Delikten.

Die zweite Komponente sind diese Massenbetrugsmails, die wahrscheinlich jeder von uns in irgendeiner Form kennt, wo es eine eigene Arbeitsgruppe gibt, die eingerichtet wurde, um diesem Phänomen zu Leibe zu rücken.

Das Dritte ist sozusagen eine spezielle Konzentration auf den Bereich des Darknets, weil das eine Organisationsdrehscheibe für die Unterstützung von allerhand kriminellen Aktivitäten ist, wo man sich Falschgeld besorgen kann, wo man sich falsche Dokumente besorgen kann, was aber auch immer mehr eine Rolle im Bereich der Drogenkriminalität spielt. Etwas überspitzt formuliert muss man sagen, der klassische Dealer, der vor der Tür steht, ist ein Auslaufmodell, so wie der klassische Buchhändler etwas ins Hintertreffen kommt, wenn ich an große internationale Versandhäuser denke, die das alles übernehmen – und ähnlich ist es im Bereich des Darknets mit den Drogen.

Präsident Mag. Wolfgang Sobotka: Zusatzfrage? – Bitte, Frau Abgeordnete.

Abgeordnete Eva-Maria Himmelbauer, BSc (ÖVP): Herr Minister! Ich möchte gleich auf einen Punkt eingehen, den Sie selbst explizit angeführt haben, das Thema Internetbetrug. Wir kennen ja alle diese Mails: hohe Gewinnversprechungen oder Erbschaften, die uns nahegelegt werden. Natürlich findet auch im Bereich des Onlinehandels sehr viel Betrug statt. Auch das entnehmen wir oft den Medien oder kennen einzelne Fälle.

Vielleicht können Sie auf diesen Bereich noch einmal genauer eingehen, welche Schritte hier von der Bundesregierung gesetzt werden, um den Internetbetrug hintanzuhalten.

Präsident Mag. Wolfgang Sobotka: Herr Bundesminister, bitte.

Bundesminister für Inneres Herbert Kickl: Internetbetrug ist ja quasi die Verlagerung des klassischen Deliktfeldes Betrug in den Bereich dieses neuen Mediums. Natürlich setzen wir da im Bereich der Ausbildung bei den Ermittlern auch entsprechend an, das heißt, wenn wir Betrugsermittler ausbilden, dann läuft immer diese Komponente der Aktivitäten im Internet entsprechend mit.

Etwas ganz Wichtiges ist ein neues Tool, das wir im Zusammenhang mit diesem Forschungsprojekt Kiras entwickeln, also im Verbund mit der Wissenschaft. Das Ganze heißt Lagebild Cybercrime, und da geht es darum, dass wir ein entsprechendes digitales Tool schaffen, das der Polizei die Möglichkeit gibt, koordinierend und steuernd im Zusammenhang mit Betrugsphänomenen im Internet vorzugehen. Man muss sich das so vorstellen, dass die Anzeigen, die ja alle in dieses allgemeine Anzeigensystem eingespeichert werden, dann, wenn sie solche Phänomene betreffen, in diesem Pool zusammenlaufen und dieses Tool dann entsprechende Gemeinsamkeiten erkennt.

Bisher ist es so, dass der eine Fall vielleicht isoliert im Burgenland ist, der andere in Vorarlberg vorkommt – so können wir aber Verbindungen herstellen, gemeinsame Muster ausforschen und damit in einer besseren Art und Weise gegen diese Täter vorgehen.

Präsident Mag. Wolfgang Sobotka: Zusatzfrage? – Bitte, Frau Abgeordnete Zadić.

Abgeordnete Dr. Alma Zadić, LL.M. (JETZT): Ich begrüße es sehr, dass Sie sich dem Kampf gegen Cybercrime verschrieben haben, denn es ist wirklich auch eine Bedrohung, die stark anwächst. Daher auch meine Frage: In etwa einem Jahr wird es möglich sein, verschlüsselte Nachrichten durch die sogenannte Spionagesoftware, den Bundestrojaner, zu überwachen. Dieser Bundestrojaner funktioniert, wenn man Sicherheitslücken eines Handys oder eines mobilen Gerätes ausnützt, die Sie kennen müssen beziehungsweise die die Softwarehersteller kennen müssen, um diese Spionagesoftware auch zu installieren.

Meine Frage: Wie wollen Sie sicherstellen, dass diese Lücken nicht von organisierten Cyberkriminellen ausgenützt werden und dass diese dadurch nicht auch die Möglichkeit bekommen, ihre eigene Spionagesoftware auf unseren Geräten zu installieren?

Präsident Mag. Wolfgang Sobotka: Herr Bundesminister, bitte.

Bundesminister für Inneres Herbert Kickl: Frau Abgeordnete! Ich muss zunächst eines richtigstellen: Ich glaube, es ist ein bisschen ein falscher Ausdruck, wenn man hier von einer Spionagesoftware spricht, das hat so ein bisschen einen anrüchigen

Touch, möchte ich fast sagen. *(Abg. **Scherak:** Das haben Sie ja auch immer gesagt!)* Das bringt eine notwendige Ermittlungsmaßnahme ein bisschen ins schiefe Licht.

Sie wissen genau, weil wir hier im Haus ausführlich über die Implementierung dieser rechtlichen Möglichkeiten diskutiert haben, dass es in Wahrheit um ein Mittel geht, das der Bekämpfung der schwersten organisierten Kriminalität und auch des internationalen Terrorismus dient und das an strengste rechtliche Auflagen gebunden ist, und daher ist nicht davon auszugehen, denn dieser Eindruck wird immer ein wenig erweckt, dass das jeder bei sich am Handy hätte. Das ist einmal eine wichtige grundlegende Vorbemerkung, weil gerne so getan wird, als ob sich jeder fürchten müsste. Fürchten müssen sich nur die Gauner, Frau Abgeordnete!

Zum Zweiten, was die Sicherheitslücken betrifft, darf ich Ihnen sagen, dass wir natürlich mit den Experten bei der Entwicklung dieser Software im Gespräch sind beziehungsweise uns Software ansehen, die ja nicht wie Sand am Meer vorhanden ist. Da gibt es wenige Produkte, die das auch tatsächlich leisten können. Nach unseren Erkenntnissen ist es so, dass diese Experten sagen, ein System, das keine Sicherheitslücken aufweist, wird es niemals geben. Das ist Wunschdenken aller Programmierer, aber das wird es nicht geben. So gesehen ist der Hinweis auf die Sicherheitslücke zwar berechtigt, aber er bringt uns jetzt nicht aus der Verlegenheit, in dem Zusammenhang trotzdem reagieren zu müssen.

Präsident Mag. Wolfgang Sobotka: Zusatzfrage? – Bitte, Herr Abgeordneter Plessl.

Abgeordneter Rudolf Plessl (SPÖ): Herr Innenminister! Der Bundesminister für Landesverteidigung ist für die Cyberdefence zuständig, Sie mit Ihrem Ministerium für Cybercrime und Cybersicherheit. Es gibt auch eine österreichische Strategie für Cybersicherheit, wo diese als Rechtsgut angeführt worden ist. Wir müssen noch große Kraftanstrengungen durchführen, damit diese Cybersicherheit auch dementsprechend für die Zukunft gewährleistet wird.

Ich möchte mich in diesem Zusammenhang betreffend die Überwachungssoftware noch einmal an Sie wenden: Auf der einen Seite gibt es eine Sicherheitslücke wie bei WhatsApp – und ich ersuche alle, die WhatsApp benützen, ein Update durchzuführen –, wo eine Privatfirma eine Sicherheitslücke entstehen hat lassen, die alle betrifft, nicht einzelne sondern alle, die dieses System benützen, und deswegen ist das Update so wichtig.

Meine Frage in diesem Zusammenhang: Es gibt eine eigene sogenannte Koordinierungsstelle, die würde gerne der Bundesminister für Landesverteidigung haben und er würde gerne auch dementsprechend federführend tätig sein. Wann und wo wird diese

Stelle eingerichtet werden, wer wird federführend sein und welche Budgetmittel – denn Sie kennen die Zahlen ja auch sehr gut vom Girls' Day, vielleicht können Sie mir da auch weiterhelfen – werden vom Bundesminister für Inneres für diese Koordinierungsstelle zur Verfügung gestellt?

Präsident Mag. Wolfgang Sobotka: Herr Bundesminister, bitte.

Bundesminister für Inneres Herbert Kickl: Danke, Herr Abgeordneter, vor allem auch vielen Dank für den Sicherheitshinweis, den Sie jetzt im Zusammenhang mit WhatsApp gegeben haben – man merkt, Sie sind ein Polizist, Ihnen geht es um die Sicherheit.

Die zweite Komponente ist: Wir sind zwar jetzt sehr, sehr beherzt am Werken, wenn es um die Frage der Umsetzung von Vorhaben im Regierungsprogramm geht, aber Sie werden Verständnis haben, dass wir nicht alles von heute auf morgen machen können. Wichtig ist, dass wir die Aktivitäten der beiden Ressorts gut miteinander verzahnen. Wer letzten Endes dann die Federführung in diesem Projekt haben wird, das traue ich mich heute noch nicht zu sagen. Sie wissen ganz genau, dass das die heißesten Eisen sind, um die es geht.

Nichtsdestoweniger werden wir die Bemühungen dahin gehend in Gang setzen, dass wir das Ziel erreichen, nämlich die Sicherheit der österreichischen Bevölkerung in diesem Bereich zu gewährleisten – und dass die Frage, wer dann dafür zuständig sein wird, eine zweitrangige sein wird. Wir werden dieses Projekt aber dann ohnehin noch im Parlament diskutieren. *(Abg. **Plessl:** Budgetmittel?!)*

Präsident Mag. Wolfgang Sobotka: Die 11. Anfrage stellt die Abgeordnete Nurten Yılmaz. – Bitte.