



„Sicherheitspolitisches Frühstück“: Hermann Feiner, BVT-Direktor Peter Gridling, Gábor Iklódy, Wilhelm Sandrisser.

## NATO, Cybersecurity, Sicherheit

**Botschafter Gábor Iklódy, Untergeneralsekretär der NATO für neue Sicherheits Herausforderungen, plädierte beim vierten „sicherheitspolitischen Frühstück“ im BMI für die Erarbeitung von Cybersecurity-Strategien.**

**G**ábor Iklódy, Assistant Secretary General der 2010 geschaffenen „Division for Emerging Security Challenges“ der NATO, war Gastreferent beim vierten „sicherheitspolitischen Frühstück“ am 4. November 2011 im Festsaal des Bundesministeriums für Inneres. Botschafter Iklódy sagte, die europäischen Staaten sollten Strategien auf dem Gebiet der Cybersecurity erarbeiten. Nur durch einen gesamtheitlichen Ansatz und den Ausbau von Kooperationen könne auf zukünftige Bedrohungen effektiv reagiert werden. Primäre Aufgabe der NATO sei es, Bedrohungen von ihren Mitgliedstaaten fernzuhalten. Geänderte Bedrohungen bedeuteten daher neue Herausforderungen; die NATO als politische Plattform könne nicht sämtliche damit verbundenen Probleme lösen, aber ein wichtiger Teil der Antwort darauf werden. So gelte es in Bereichen wie Cyber-Angriffen, Energie- und Umweltfragen sowie strategischer Vorausschau Entwicklungen vorherzusehen, um Kri-

sen rechtzeitig verhindern zu können. Von essenzieller Bedeutung sei eine gute Zusammenarbeit der Nationalstaaten unter Einbindung der Zivilgesellschaft, aber auch die internationaler Organisationen, die verbesserungswürdig sei. Nur so könnten Erkenntnisse ausgetauscht und Doppelgleisigkeiten verhindert werden.

**In der Terrorismusbekämpfung** seien die Kernelemente der NATO-Strategie Vorbeugung und Bekämpfung. Da kein Land immun gegen Terrorismus sei, müsse die Zusammenarbeit intensiviert werden. Um den Bereich der Abschreckung besser zur Geltung zu bringen, könne man nur versuchen, den potenziellen Mehrwert eines Angriffs zu verringern. Zur effektiveren Bekämpfung sei eine eindeutige Klärung der Verantwortlichkeiten auf staatlicher Ebene nötig.

Die traditionelle Trennung von Verteidigung und innerer Sicherheit wirke sich einschränkend auf diverse sicher-

heitsrelevante Fähigkeiten aus. Iklódy plädierte für eine stärkere Zusammenarbeit dieser Bereiche.

Eine Kernaufgabe der NATO sei es, die bündniseigenen Netze und Infrastrukturen zu schützen sowie jene der Mitgliedstaaten, von denen die NATO abhängig sei. Zu den traditionellen Angriffsräumen (Luft, Land, See) sei ein weiterer hinzugekommen – der Cyber-Raum. Hier müsse die NATO bereit sein zu helfen, zu verteidigen und – wenn notwendig – zu kontern.

Die Aufgabe der NATO zum Schutz kritischer Infrastruktur sei die Entwicklung von Mindeststandards für die Staaten auf den Gebieten Bekämpfung und rasche Reaktions-/Erholungsfähigkeit. Hier und in den Themenfeldern Energiesicherheit und Weiterverbreitung von Massenvernichtungswaffen liege die Stärke der NATO im Aufbau von Kapazitäten und im Erfahrungsaustausch. Schutzaufgaben auf dem Gebiet der Energiesicherheit zu übernehmen, sah Iklódy weniger als Auf-

trag an die NATO. Die teils sehr ambitionierten Strategien müssten von den Mitgliedstaaten auch umgesetzt werden. Als Prioritäten-Regionen für die NATO-Sicherheitspolitik strich Iklódy Asien hervor – vor allem Afghanistan und den Iran und sein Umfeld, sowie den Westbalkan und den MENA-Raum. Hier wären Partnerschaften von besonderer Bedeutung, Österreich mit seinen Erfahrungen und seiner Expertise am Balkan sei ein wichtiger Partner.

**Cybersecurity.** In Bezug auf die Zukunft der Cybersecurity betonte der Referent die Verantwortung der Staaten, von deren Territorien Cyber-Angriffe gestartet werden, die Intensivierung der Kooperation mit Unternehmen und Industrie und das Einholen von Expertenwissen aus diversen gesellschaftlichen Bereichen. Man dürfe auch den Schaden für die Volkswirtschaften nicht unterschätzen, ein Trend, der sich noch verstärken werde. Grundsätzlich seien Verhaltensregeln (Norms of Behaviour) auf internationaler Ebene zu entwickeln, denen die Akteure folgen sollten. Die diesbezüglichen Initiativen diverser internationaler Organisationen seien zu begrüßen, je-



**Gábor Iklódy: „In Bereichen wie Cyber-Angriffen gilt es, Entwicklungen vorherzusehen, um Krisen rechtzeitig verhindern zu können.“**

doch gab Iklódy zu bedenken, dass diese Organisationen lediglich Instrumente der Staaten seien, die heute nicht gut genug genutzt würden. Man könnte weit bessere Ergebnisse erzielen. Erforderlich hierzu seien Verhandlungsergebnisse zwischen den Staaten.

In der Podiumsrunde strich Sektionschef Hermann Feiner, Leiter der Sektion IV, die Komplexität der behan-

delten Themen hervor. Die Bewältigung der Herausforderungen und die Entwicklung von Gegenstrategien gegen Instabilitäten seien das Gebot der Stunde. Österreich und das BMI würden sich an diesem Prozess beteiligen.

Mag. Peter Gridling, Direktor des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung, wies auf das Problemfeld der Erzeugung von Abwehrfähigkeit in einem scheinbar sicheren Umfeld hin. Jede Organisation sei aufgerufen, sich mit dem Thema Cybersecurity auseinanderzusetzen, ein Informationsaustausch sollte umfassend stattfinden. Die politische Ebene sei aufgerufen zu reagieren. Gesetzliche Regelungen seien schwierig aber notwendig. Der erste Schritt zur Cyber-Verteidigung starte bei jedem Nutzer zu Hause beim privaten Computer und im eigenen System.

In seiner Zusammenfassung betonte Dr. Wilhelm Sandrissler, Leiter der Gruppe I/B, die Notwendigkeit eines gemeinsamen Vorgehens innerhalb der Nationalstaaten und im internationalen Umfeld. Österreich werde sich seiner Verantwortung stellen und bereitwillig kooperieren.

*Benedikt Hensellek/Nieves Kautny*

INTERPOL

**Weltweites Service**

Zahlreiche Interessierte aus dem In- und Ausland nahmen vom 5. bis 7. Dezember 2011 im Bundeskriminalamt in Wien an einer Interpol-Awareness-Veranstaltung teil.

Ziel der Veranstaltung war die Information über die Möglichkeiten und Ressourcen Interpols zur Bekämpfung der nationalen und internationalen Kriminalität. Durch die optimale Nutzung des Interpol-Netzwerks sollen die Aktions- und Reaktionszeiten der Behörden verkürzt werden. Einen erheblichen Beitrag dazu leistet der internationale polizeiliche Daten- und Informationsaustausch.

Hochrangige Vertreter des Interpol-Generalsekretariats in Lyon sowie Experten aus Österreich hielten Vorträge. Dazu kamen praxisorientierte Workshops zu den Themen DNA, Wirtschaftskriminalität und Hightech-Crime sowie Menschenhandel und Schlepperei. Vorgestellt wurde unter anderem das *Command and Co-Ordination*



**Hakan Erdal (Interpol), BK-Direktor Franz Lang, Catherine Plano (Interpol), GD Herbert Anderl, Ursula Neder (Interpol), Thomas Herko (BK), Sergio di Pasquale (Interpol), Clemens Wechner (Interpol).**

*ation Centre (CCC)* und das Kommunikationssystem „I-Link“ sowie andere Angebote Interpols.

„Interpol vereinigt als einziger weltweiter Polizeiverband bereits 190 Mitgliedstaaten und ist durch diese

Vernetzung von großer Bedeutung für die Verfolgung und Bekämpfung der internationalen grenzüberschreitenden Kriminalität“, betonte der Generaldirektor für die öffentliche Sicherheit, Dr. Herbert Anderl, bei der Eröffnung.

FOTOS: ALEXANDER TUMA, BK/JOHANN FRASL