Konferenz LIPS / SPFZ

„Risiken des Internets – Herausforderung für Politik, Wirtschaft und Gesellschaft“

Freitag, 16. November 2012, 13.30–17.30 Uhr
Hotel Schweizerhof Luzern

Konferenzbericht

Risiken des Internets

Die Risiken des Internets für Politik, Wirtschaft und Gesellschaft standen im Mittelpunkt der diesjährigen Konferenz zur öffentlichen Sicherheit, die von der Lucerne Initiative for Peace and Security (LIPS) wiederum zusammen mit dem Sicherheitspolitischen Forum Zentralschweiz organisiert worden war. Den Schwerpunkt bildeten Referate zur nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken, zur Internetkriminalität sowie zur Bedrohung kritischer Infrastrukturen. Die Konferenz wurde mit einer Podiumsdiskussion namhafter Persönlichkeiten aus Politik, Verwaltung und Wirtschaft abgerundet.

Dr. Bernhard Wigger, Präsident der Luzerner Initiative für Frieden und Sicherheit, wies in seiner einleitenden Rede darauf hin, dass sich die heutigen Sicherheitsüberlegungen nicht mehr lediglich auf die physische Gewalt konzentrieren, sondern künftig auch der Cyber-Raum als Projektionsfläche für Angriffe eine strategische sicherheitspolitische Bedeutung hat. Die Konferenz stand im Zeichen dieser neuen, aktuellsten Sicherheitsbedrohung; einerseits, um das Publikum zu sensibilisieren, andererseits, um die diesbezüglichen Bedürfnisse seitens Politik, Verwaltung und Wirtschaft aufzuzeigen. Bernhard Wigger plädierte für eine Zusammenarbeit in der Bewältigung der eher neuen Bedrohungsform. Im Sicherheitsverbund Schweiz (SVS) wird sich künftig eine Fachgruppe „Cyber-Risiken“, die aus Vertretern des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS), der Kantone und der Privatwirtschaft zusammengesetzt ist, mit Cyber-Risiken befassen.

Pietro Donzelli, Präsident des Sicherheitspolitischen Forums Zentralschweiz, forderte eine gemeinsame kohärente Strategie, um die Risiken des Internets zu minimieren. Es sei nicht nur das Interesse des Bundes, sondern auch der Kantone sowie der privaten Nutzer, sich gegen die Risiken aus dem Internet zu schützen. Für ihn steht fest: Die Tatsache, dass keine Bundesrätin bzw. kein Bundesrat an der diesjährigen Konferenz teilgenommen hat, weise auf das Fehlen einer eindeutigen Zuständigkeit in diesem Politikbereich hin. Zwar habe der Bundesrat eine nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken verabschiedet, sichtbar sei diese aber noch nicht.

Yvonne Schärli-Gerig, Regierungspräsidentin des Kantons Luzern und Präsidentin der Schweizerischen Kriminalprävention, betonte in ihrer Begrüssungsrede, dass die Internetkriminalität ernst genommen werden müsse. Gerade weil die Internetkriminalität ein noch unbekanntes Ausmass annehmen könnte, sei es wichtig, aufzuklären und Anlaufstellen für Betroffene zu schaffen.

Peter Fischer, Delegierter für die Informatiksteuerung des Bundes, stellte in seinem Referat die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken vor. Er sprach sich für eigenverantwortliches Handeln im Umgang mit dem Internet aus. Es sei artfremd, die Zuständigkeiten für das Internet einer einzigen zentralen Stelle oder einem Departement zuzutragen, denn das „Internet gibt es überall". Ein Grossteil der Bevölkerung habe heutzutage Internetanschluss und brauche tagtäglich die Informations- und Kommunikationstechnologien (IKT). Dies gehe aber gleichzeitig mit einer erhöhten Interdependenz der kritischen Infrastrukturen einher. Peter Fischer wies darauf hin, dass die IKT entscheidend für den Schweizer Standortwettbewerb, für Wachstum und Innovation sind. Gemäss Peter Fischer gibt es eine breite Bedrohungslage: politische Aktivisten, organisierte Kriminalität, Wirtschaftsspionage, Sabotage, Diebstahl von elektronischen Identitäten etc. Die Cyber-Strategie habe zum Ziel, die Risiken frühzeitig zu erkennen, die Widerstandsfähigkeit zu erhöhen und die Cyber-Risiken zu reduzieren. Er plädierte für eine Gesamtanalyse und Zusammenarbeit verschiedener Akteure. Es brauche ein verstärktes und verbessertes Krisenmanagement, die betroffenen Akteure sollten sich besser vernetzen. Die Cyber-Strategie sieht vor, die darin vorgeschlagenen Massnahmen entlang der Handlungsfelder bis 2017 vorzunehmen.

Martin Boess, Geschäftsleiter der Schweizerischen Kriminalprävention (SKP), referierte zum Thema „Internetkriminalität – der virtuelle Tatort mit realen Auswirkungen auf Bürgerinnen und Bürger". In seinem Referat appellierte er an die Verantwortung im Umgang mit dem Internet und forderte eine gewisse Medienkompetenz, also das Wissen, wie das Internet verantwortungsbewusst gebraucht werden kann. Er machte darauf aufmerksam, dass die Kriminalprävention nicht nur die Aufgabe der Polizei sei, sondern auch die Schule und die Gesellschaft involviert werden müssen. Das Internet hat ein enormes Ausmass angenommen, gab es 1996 noch 250 000 Webseiten weltweit, so sind es heute mehr als 17 Milliarden Webseiten. Wir werden als „Prosumer" bezeichnet, eine Zusammensetzung aus den Wörtern Produzent und Konsument. Einerseits wird konsumiert, andererseits kann durch das Hochladen von (persönlichen) Informationen auch produziert werden. Mithilfe sozialer Netzwerke können wir Informationen ins Netz stellen. Gemäss Boess „hat eine Demokratisierung stattgefunden" und „jeder kann

auf dem Internet mitmachen, man braucht kein Technikfreak zu sein“. Das Internet stehe somit u. a. „Kriminellen, Naiven, Gierigen, Einsamen“. zur Verfügung. Dadurch gebe es auch viele Möglichkeiten, Delikte zu begehen und Opfer zu werden. Da „das Internet zur Entwertung des Expertentums geführt“ habe, könne nicht allem getraut werden, was ins Internet gestellt werde. Schützen vor „Cybergrooming“, „Cybermobbing“ und „Cyberstalking“ könne man sich mit Misstrauen, sparsamem Umgehen mit persönlichen Daten im Internet und guten Sicherheitseinstellungen des Profils in sozialen Netzwerken.

Nationalrätin **Barbara Schmid-Federer**, die sehr kurzfristig ihren Auftritt absagen musste, stellte jedoch ihre Präsentation „Herausforderungen für die Cyber-Generation“ zur Veröffentlichung auf der LIPS-Homepage zur Verfügung. Derzufolge will sie mit einer von ihr eingereichten Motion, die neuen Phänomene des Internets betreffend, gegen das Grooming vorgehen, also gegen das gezielte Ansprechen von Personen im Internet mit dem Ziel der Anbahnung sexueller Kontakte. Ihr Ziel ist es, Grooming strafgesetzlich zu ahnden. Schmid-Federer findet, dass wir alle zur Cyber-Generation gehören. Der Cyberspace verbirgt mehrere Risiken, so wurde Schmid-Federer selbst Opfer eines „Shitstorm“, der eine neue Form des Cyber-Mobbing darstellt. Von „Shitstorm“ sind sowohl Individuen, Firmen, Organisationen, wie auch Staaten betroffen. Auch wenn, so Schmid-Federer, Shitstorm und Bullying Offizialdelikte sind, genüge eine Strafanzeige nicht, um das Problem zu lösen. „Der Cyberspace fordert von uns allen, die ihn erleben, unser Bestes zu geben, in ihm mehr zu sehen als nur ein Spielfeld der Eitelkeit und des persönlichen Gewinns.“ Ein umfassender Ansatz sei hier gefragt.

Andy Mülheim, Bereichsleiter Informatik und Sicherheit von swissgrid, referierte zum Thema „Die Bedrohung kritischer Infrastrukturen durch Cyberwar“. Kritische Infrastrukturen (KI) erbringen Dienstleistungen, welche für den Staat, die Gesellschaft unabdingbar sind. Dies sind beispielsweise Energie- und Wasserversorgung, Elektrizität und Verkehr. Sie sind verantwortlich für das Funktionieren des öffentlichen Lebens und bilden die Basis, auf welcher sich eine Gesellschaft weiterentwickeln kann. Ein Angriff auf KI schadet dem Staat bzw. der Gesellschaft als Ganzer. Andy Mülheim wies darauf hin, dass der Ausfall einer KI einen Dominoeffekt auf andere KI haben könnte. Das Bundesamt für Energie schätzt bei einem Ausfall des Stromnetzes die Kosten auf 8–30 Mio. Franken pro Minute. Gemäss Andy Mülheim nehmen technische Gefährdungen und Bedrohungen gerade wegen zunehmender Vernetzung und Zentralisierung der KI und ihrer Steuersysteme zu. Er geht davon aus, dass die zunehmende Komplexität der Technologien den Cyberraum stark verändert hat. „Kritische Infrastrukturen sind sehr wohl durch Cyberwar bedroht“. Andy Mülheim wies auf das fehlende Verständnis für die neue Bedrohungsform und die damit verbundenen sicherheitsrelevanten Fragen hin. Die Nutzer von KI, so Mülheim, haben eine Erwartungshaltung, sie wollen für die Leistungen immer weniger bezahlen. Dadurch können notwendige Sicherheitsinvestitionen kaum oder nur ungenügend getätigt werden. Die Basisleistungen von KI seien für alle selbstverständlich, man gehe davon aus, dass alles immer funktioniere. Eine wirksame „Cyberdefence“ brauche eine verbesserte Zusammenarbeit zwischen den öffentlichen Behörden und dem privaten Sektor. Die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken stehe

vor der Herausforderung, sowohl Staat als auch Betreiber zu involvieren und gemeinsam gegen Cyberwar anzukämpfen.

Zur **Podiumsdiskussion** fanden Experten aus Politik, Verwaltung und Wirtschaft zusammen. Unter der ausgezeichneten, lebhaften und kompetenten Moderation von **Mark Saxer**, Geschäftsführer Swiss Police ICT, diskutierten sie Fragen zum Thema Hackerangriffe, Cyberwar und Aufgaben der verschiedenen Akteure. **Ivan Bütler**, Geschäftsleiter von Compass Security betonte, dass das Antizipieren von Angriffen wichtig sei. Verteidigen könne man nur, wenn man wisse, wie zu verteidigen sei und gegen wen man sich verteidigen müsse. Er erwähnte in diesem Zusammenhang das Land Österreich, welches einen Wettbewerb als Nachwuchsprogramm für künftige Cyberspezialisten organisierte. Dies zeige insbesondere auf, dass der politische Wille da sei, um sich nachhaltig gegen Cyberangriffe zu schützen. Mit **André Duvillard**, Delegierter Bund und Kantone für den Sicherheitsverbund Schweiz (SVS), gingen die Referenten einig, dass Politik und Justiz technologischen Entwicklungen hinterherhinken. Die Kantone hätten zudem wenig Mittel und Ressourcen, um dieser Problematik wirksam entgegenzuwirken. Die Podiumsteilnehmer pflichteten André Duvillard bei, dass nur gemeinsam effektiv gegen Internetkriminalität vorgegangen werden könne. Dabei sei es wichtig, dass die Betreiber von kritischen Infrastrukturen, wie beispielsweise swissgrid, bei der Umsetzung der Cyberstrategie von Anfang an mit einbezogen werden. Alt-Nationalrat und Informatiker **Christoph von Rotz** sprach sich dafür aus, dass Unternehmen ihre Verantwortung besser wahrnehmen, indem sie kontinuierlich Risikoanalysen tätigen. Laut **Marc Henauer**, Leiter des Operations- und Informationszentrums bei der Melde- und Analysestelle Informationssicherung (MELANI), werden staatliche oder staatlich unterstützte Angriffe nicht nur dort begangen, wo man verletzlich ist; Attacken finden auch dort statt, wo sie nicht vermutet werden. **Ivan Bütler** vertrat die Meinung, dass „Cyberkrieg“ als solcher nicht existiere. Auch **Marc Henauer** fügte an, dass mit dem Begriff Cyberwar meistens Spionage gemeint sei; der Imageschaden eines Unternehmens oder der Verwaltung bestehe darin, dass Daten illegal geflossen sind. Ein weiterer Grund der Verletzlichkeit von Unternehmen besteht gemäss **Ivan Bütler** darin, dass am Arbeitsplatz Smartphones und soziale Netzwerke benutzt

werden dürfen. Mit der Idee, die Zufriedenheit der Mitarbeitenden zu gewährleisten, werden Türen für einen Cyberangriff geöffnet.

Schlussfolgerungen aus der Konferenz

Die nationale Strategie zum Schutz vor Cyber-Risiken darf kein Papiertiger bleiben. Die Verantwortlichkeiten sind stufengerecht zu regeln und die dafür notwendigen personellen Ressourcen zur Verfügung zu stellen. Aus den Referaten und der Podiumsdiskussion ging klar hervor, dass den Cyber-Risiken noch nicht genügend Aufmerksamkeit geschenkt wird. Die Quintessenz unserer Konferenz war, dass sich die Bevölkerung und die Politik der Bedrohungslage und des enormen Schadenpotenzials noch zu wenig bewusst sind. Die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken muss rasch sichtbar und wirksam werden, um die Bevölkerung und ihre Wirtschaft angemessen schützen zu können. Dabei kann von den Erfahrungen anderer Länder, wie etwa Österreich, gelernt werden.

Die Veranstalter

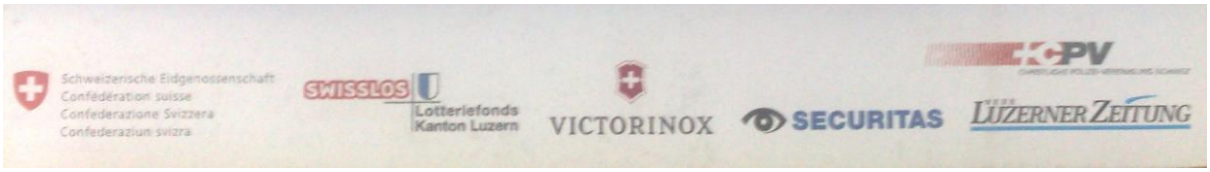
Die Konferenz zu den Risiken des Internets wurde von der Lucerne Initiative for Peace and Security (LIPS) und dem Sicherheitspolitischen Forum Zentralschweiz organisiert.

LIPS
lucerne initiative for peace and security

Sicherheitspolitisches
Forum Zentralschweiz

Sponsoren

Die Konferenzveranstalter möchten den Sponsoren, die diesen Anlass ermöglicht haben, auch an dieser Stelle herzlich danken**:**



Kontakt

LIPS – Lucerne Initiative for Peace and Security
Postfach 3303
CH-6002 Luzern
+41 (0)79 239 44 91 (Dr. Bernhard Wigger)
info@lips-org.ch │ www.lips-org.ch