

Cyberkriminalität greift um sich : wie bekämpfen?

Autor(en): **Heim, Karl J.**

Objektyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **181 (2015)**

Heft 10

PDF erstellt am: **18.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-583241>

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Cyberkriminalität greift um sich – wie bekämpfen?

Das 14. Forum «Innere Sicherheit» des Verbandes Schweizerischer Polizei-Beamter (VSPB) gab am 24. Juni 2015 im Schluss-Communiqué eine Antwort: «Ressourcen und Ausbildung sind das Problem». Zu ergänzen ist die Notwendigkeit einer effizienteren föderalistischen Zusammenarbeit. Mit verschärften Gesetzen allein ist es nicht getan.

Karl J. Heim

Hochkarätig war die Runde der Referenten, die der VSPB zu dieser aktuellen, sich rasend schnell weiter entwickelnden Problematik einlud: Neben Bundesanwalt Michael Lauber steuerten u.a. Nationalrätin Corina Eichenberger als Vizepräsidentin der Sicherheitspolitischen Kommission des Nationalrates (SiK-N), Stefan Blättler, Kommandant der Kantonspolizei Bern, und Sébastien Fanti, Datenschutz- und Öffentlichkeitsbeauftragter des Kantons Wallis, ihre Voten bei. Die Wissenschaft war durch einen Experten für digitale Medien, Professor Werner Hartmann, vertreten. Die Quintessenz aller Aussagen war klar: Cyberkriminalität greift in sämtliche gesellschaftliche Belange ein, und – sie ist äusserst schwer aus der Welt zu schaffen. Denn:

«Einmal im Netz, immer im Netz!»

Mittlerweile gibt es zahllose Beispiele dafür, wie einfach Kriminelle im digitalen Raum ans Ziel kommen. So können gefälschte Facebook-Einträge den Inhaber einer Seite überraschend in grösste Schwierigkeiten bringen. Schon hier zeigt sich, dass das geltende Recht an seine Grenzen stösst. Denn gegen solche Machenschaften nützt ein Anspruch auf Löschung oder Vergessen rein gar nichts. Zwar ist es trivial, soll aber dennoch wiederholt werden: Je mehr das ahnungslose Individuum auf den ihm offen stehenden digitalen Kanälen von sich preisgibt, desto unvermittelter und brutaler ist es angreifbar! So reichen vier über den Tag verteilte Ortsangaben des eigenen Handys bequem, um jemanden zweifelsfrei und umfassend zu identifizieren. Cybermobbing, Phishing-Mails und der gezielte anonyme Aufruf zu Krawal-

len (mit grosser Resonanz!) sind weiteres, heute schon stark genutztes «Tafelsilber» aus dem Giftschrank der Digitalkriminellen. Eine laufend grösser werdende Kluft zwischen aktueller Gesetzgebung

Diskussionsrunde mit (von links) Datenschützer Sébastien Fanti, Polizeikommandant Stefan Blättler, Moderator Adrian Plachesi, Nationalrätin Corina Eichenberger, Bundesanwalt Michael Lauber. Bild: VSPB



Flut cyberkrimineller Phänomene

Die so sehr geschätzte Erleichterung der täglichen Kommunikation kann bei schon kleinsten Unachtsamkeiten leicht

zum Verhängnis werden. Von wissenschaftlicher Seite kommt die klare Aussage, dass allgemein die Komplexität der heutigen vernetzten Welt, wenn nicht glatt

«Der Faktor Mensch ist bei der Aufklärung dieser Kriminalität entscheidend – und die Bundesanwaltschaft ist personell rasch mit den notwendigen Mitteln auszustatten.»

ignoriert, so doch stark unterschätzt wird und von der Gesellschaft kaum ins reale Bewusstsein gerückt worden ist. Hier haben kantonale Polizeivertreter und die Bundesanwaltschaft bei der – höchst un-

befriedigenden – Tatsache ein, dass für sie als Schutzinstanzen der Gesellschaft mit Verfassungsauftrag der Zugriff auf wichtige Daten nicht gewährleistet oder nur schwer nach langwierigen Prozeduren möglich wird – wenn es vielleicht schon zu spät ist.

Gemäss Lauber liegen grosse Gefahren in den Vorbereitungs- und Propaganda-Handlungen terroristischer Aktionen, welche sich – wie im Fall des Islamischen Staats unterdessen fast täglich den Medien zu entnehmen ist – weitgehend in den digitalen Raum verlagert haben. Der verhältnismässig sehr geringe Aufwand steht dabei im umgekehrten Verhältnis zum schwer abschätzbaren Erfolg. Ausgeklügelte kryptische Verschlüsselungsmethoden kommen der Anonymität entgegen und erschweren in grossem Umfang eine adäquate Aufklärung.

Dennoch ist der Bundesanwalt nicht prioritär mit dem Instrumentarium des geltenden Rechts unzufrieden, als Wink an das Parlament befürchtet er aber, dass in der Bevölkerung das diffuse Gefühl von rechtsfreien Räumen entstehen könnte. In diesem Sinne muss sich die Gesetzgebung auf das Wesentliche beschränken: wegen der Kleinheit der Schweiz im globalen Kontext bedeutet dies u.a. die Schaffung griffigerer und effizienterer juristischer Rahmenbedingungen für die internationale Zusammenarbeit.

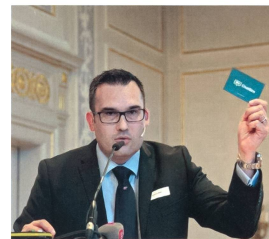
Als eines von mehreren Beispielen nahm Lauber auf das Phishing-Phänomen Bezug und nannte die jährliche Zahl von gegen 20000 betroffenen Kreditkarten, womit sich hoch spezialisierte Mitarbeiter der Bundeskriminalpolizei herumschlagen. Vor diesem Hintergrund wird zweierlei klar: Der Faktor Mensch ist bei der Aufklärung dieser rasant zunehmenden Kriminalität entscheidend – und die Bundesanwaltschaft ist daher auch personell rasch mit den notwendigen Mitteln besser auszustatten.

Komplexe Herausforderungen

Ähnlich präsentiert sich die Situation aus der Sicht der kantonalen Polizeibehörden. Als Kommandant der Berner Kantonspolizei, mehr aber noch als Präsident der Konferenz der kantonalen Polizeikommandanten, nannte Blättler die Dinge (sprich: die grossen Baustellen) unverblümt beim Namen: Weil Schnelligkeit, hohe Reichweite, Unkontrollierbarkeit und Anonymität des Internets

die Polizei vor ganz neue Herausforderungen stellen, sind für die Strafverfolgung hohe technische Kenntnisse unabdingbar, um die komplexe Materie der Cyberkriminalität erfassen und bekämpfen zu können.

In den Sozialen Medien (welche zu grossen Teilen Ursprung und Zielscheibe digital-krimineller Aktivitäten sind) sieht



Sébastien Fanti



Sébastien Fanti, Datenschutzbeauftragter des Kantons Wallis, erläutert die Phishing-Problematik. Bild: VSPB

Blättler bedeutende Chancen für die Aufklärungsarbeit. Vonseiten der kantonalen Polizeikörper erwartet er in diesem schnell wachsenden Bereich primär eine Bündelung der Kräfte und einen noch gezielteren Einsatz. Dabei geht es nicht zuletzt darum, den «Feind» gleichsam mit seinen eigenen Waffen zu schlagen: zum Beispiel auf den Sozialen Medien beim Aufdecken falscher Gerüchte gezielt deskalierend zu wirken.

Zwar genügt die polizeiliche Generalklausel in der Verfassung zur Bekämpfung dieser neuen Kriminalitätsformen bei weitem nicht mehr – dennoch ist auf politischer Ebene nicht zuerst die Gesetzgebung bei Bund und Kantonen auszubauen. Was nottut, ist eine noch engere horizontale Kooperation unter den kantona-

Nationalrätin Corina Eichenberger: Unterschätzen wir die Gefahren nicht!

Interview Karl J. Heim

Frau Nationalrätin, welche Kriminalität im Netz ist für Sie die wichtigste?

Ich möchte mehrere nennen, auf gleicher Stufe: Wirtschaftlicher Nachrichtendienst, verbotener Nachrichtendienst, Vorbereitung terroristischer Angriffe auf Menschen und Infrastrukturen – sowie natürlich Betrügereien aller Art.

Zu den dunklen Seiten von Social Medias: Aus ursprünglich harmlosen Dialogen können sehr schnell Erpressungsversuche und sogar sexuelle Übergriffe werden. Wie Gegensteuer geben?

Von den «Social Natives» zu den «Social Naives»; hier ist der Staat mit seinen Mitteln besonders gefordert, denn es geht zu einem grossen Teil um den entscheidenden Schutz von Jugendlichen und jungen Erwachsenen. Im Parlament wurde diese Problematik bereits 1996 thematisiert. Ich bin daher sehr froh, dass seit 2002 in Chaträumen verdeckt ermittelt werden kann, z. B. durch die Kantonspolizei Zürich.

Sie haben ja in Ihren Ausführungen auch das BÜPF (Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs) angesprochen. Sehen Sie dort kein Missbrauchspotenzial oder Übereifer der Behörden?

Das neue Gesetz will ja die Überwachungsmöglichkeiten der Strafverfolgungsbehörden an neue technische Gegebenheiten



anpassen, was angesichts der aktuellen Entwicklungen nur folgerichtig ist. Sowohl die vorgesehene längere Vorratsdatenspeicherung (neu: ein ganzes statt ein halbes Jahr) als auch der mögliche Einsatz von «Staatstrojanern» sind an

sehr restriktive Regelungen richterlicher Ermächtigung gebunden. Insofern sehe ich keine Schwierigkeiten, weil der Nutzen im Interesse von Staat und Bürger klar überwiegt.

Zu der von Ihnen geschilderten Zusammenarbeit von MELANI (Melde- und Analysestelle Informationssicherung des Bundes) mit den Swiss Cyber Experts, unterstützt von Polizeiorganen, dem VBS und dem EFD: Sind nicht etwas viele Partner beteiligt?

Nein, das glaube ich nicht. Denn federführend ist ganz klar MELANI. Die Meldestelle kann aber nicht alles selber machen, sie ist auf Koordination und Unterstützung der anderen genannten Behörden in Bund und von grossen kantonalen Polizeikörpern

angewiesen – gerade auch für Austausch und Bearbeitung wissenschaftlicher Daten.

Frau Nationalrätin, ich danke Ihnen für das Gespräch.

len Polizeikörpern und vertikal der Justizbehörden des Bundes mit den Spezialisten in den Kantonen.

Staatspolitisch wo ansetzen?

Es ist die Ebene der Kantone, wo die Behörden wie an einer Front mit den verheerendsten Auswüchsen der Cyberkriminalität konfrontiert sind, weil sie oft die Schwächsten trifft und ihnen nebst materiellen mitunter auch bleibende psychische Schäden zufügt. Fanti ist Rechtsanwalt und Datenschutzbeauftragter des Kantons Wallis. Wohl aufgeschreckt durch das hohe Mass an krimineller Energie, welches von perfekt verschlüsselten «Silent phones» über den illegalen Import von 50(!) Drohnen und sogenannter «Sextorsion» (auf das Intim-

und Sexualleben zielende Erpressungsversuche) seine Wirkung entlädt, sieht er die Bekämpfungsmöglichkeit innerhalb der Kantons- und Landesgrenzen längst erschöpft, ja zur Unwirksamkeit verdammt. Er fordert daher rigoros, die Sozialen Netzwerke unter Druck zu setzen – was aber in seiner Optik nur mit strafferer und fokussierterer Gesetzgebung funktionieren kann.

Wie der Bundesanwalt verlangt der kantonale Datenschützer ein vermehrtes und überzeugtes Denken «out of the box». Nur zeigt sich eine – erhebliche – Diskrepanz darin, dass offenbar die Wahrnehmung in einzelnen Kantonen und beim Bund unterschiedlich ist, was die effizientesten Methoden und die optimale Gesetzgebung für den Kampf gegen Cyberkriminalität betrifft.

Während der Kommandant der Berner Kantonspolizei eher der Meinung des Bundesanwalts zuneigt, wonach es sowohl in den Kantonen wie beim Bund besser ausgebildete Spezialeinheiten braucht (technisch auf Augenhöhe mit den Akteuren der illegalen Seite) und eine überhastete Legiferierung kaum Remedur schaffen würde, setzt der Walliser Datenschutzbeauftragte klar auf das Pferd umfassender rechtlicher Rahmenbedingungen. Diese erwartet er von der Bundesebene: Das Parlament muss in seinen Augen die Voraussetzungen schaffen, eine Spezialisierung und Zentralisierung der Kräfte im Kampf gegen diese Formen der Kriminalität in einer einzigen «Cyber Crime Unit» mit Sonder-Cyberstaatsanwälten einzurichten.

«Cyber Crime Experts» braucht das Land!

Auch aus juristischer und staatspolitischer Sicht ist das Öffnen der legislativen Schleusen wohl kaum das allein Seligmachende. Es war Eichenberger, welche gerade in ihrer Eigenschaft als Vizepräsidentin der Sicherheitspolitischen Kommission vor übereilter neuer Regulierung warnte. Als Parlamentarierin an vorderster Front der Gesetzgebung machte sie klar, dass Erlasse zwangsläufig und ständig gegenüber der äusserst hohen Kreativität der Cyberkriminellen ins Hintertreffen geraten. Entscheidend ist hier die Griffbarkeit der Regelungen.

Mit einer eigenen Motion fordert sie den Bundesrat zu Recht auf, in Abstimmung mit der Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren ein reaktionsschnelles und schlankes Netz von polizeilichen Kompetenzzentren gegen die Auswüchse der Cyberkriminalität einzurichten – und zwar unter Beizug sogenannter «Swiss Cyber Experts». Eine brillante Idee, doch die Parlamentarierin zeigt sich desillusioniert,

sieht doch der Bundesrat eine Lösung für das von ihr formulierte Problem erst – im Jahr 2031. Ein weiteres Indiz dafür, dass auch im sicherheitspolitischen Bereich

«Schnelligkeit, höchste technische Kompetenz und Handlungsfreiheit dürften im cyberkriminellen «Business» die für den Erfolg entscheidenden Hebel der Polizei sein.»

zunächst die föderalistische Zusammenarbeit gestärkt werden muss.

Wesentlich um diese Diskrepanzen gruppierten sich in der Experten-Diskussionsrunde die Themen im Kontext von Cyberverbrechen. Einig war man sich darin, dass entscheidende Fortschritte gemacht werden müssten, um dieser rasant,

ja teilweise furchterregend rasch wachsenden Welt der digitalen Kriminalität Herr zu werden. Ob dies durch noch umfassendere Gesetzgebung, durch vermehrte Zentralisierung (mittels föderalistischer, kompetenzerweiternder Zusammenarbeit) oder fallweise durch starke technische Unterstützung der Kantone vonseiten des Bundes geschehen soll – daran scheiden sich die Geister. Das Eine tun und das Andere nicht lassen, wäre man wohl aufgrund aller in Referaten und Diskussionen gefallenen Voten versucht zu sagen. Rasch und ganz ohne faule Kompromisse – denn Schnelligkeit, höchste technische Kompetenz und Handlungsfreiheit dürften im cyberkriminellen «Business» die für den Erfolg entscheidenden Hebel der Polizei sein. ■



Oberstlt
Karl J. Heim
Think Tank HKA
lic. iur. Executive MBA FH
Rechtsdozent
4102 Binningen



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS
armasuisse
Kompetenzbereich Landssysteme

PROJEKTLEITER/IN ARTILLERIESYSTEME IM BEREICH LANDSYSTEME SCHWER 80–100 % / ARBEITSORT: BERN



armasuisse ist das Kompetenzzentrum des Bundes für die Beschaffung von komplexen und sicherheitsrelevanten Systemen und Gütern sowie für das Technologie- und Immobilienmanagement.

Ihre Aufgaben

- Zeitgerechte und wirtschaftliche Abwicklung der Projekte von Artilleriesystemen
- Technische Bearbeitung während der Evaluation, Beschaffung und dem Änderungsdienst
- Verhandeln mit Auftraggebern, Nutzern, Leistungserbringern und Industrie im In- und Ausland
- Erstellen technischer Anforderungen, Ausschreibungsunterlagen, Nutzwertanalysen und Berichte

Ihre Kompetenzen

- Studium als Ingenieur/in ETH oder FH (Maschinen- oder Elektrotechnik) und BWL-Weiterbildung
- Mehrjährige Erfahrung in Entwicklungs- oder Beschaffungsprojekten
- Team- und lösungsorientiert, verhandlungssicher und durchsetzungsfähig
- Idealerweise Milizoffizier der Artillerie, fundierte Kenntnisse der Feuerleit- und Waffentechnik
- Aktive Kenntnisse in zwei Amtssprachen sowie sehr gute Englischkenntnisse
- Bewerbungen aus der romanischen Sprachgemeinschaft sind besonders erwünscht

Onlinebewerbungen unter www.stellen.admin.ch, Ref. 25342, bis **18. Oktober 2015**
Kontaktperson: Frau Brigitte Utiger, Personalleiterin, Tel. 058 464 56 90

Weitere interessante Stellenangebote der Bundesverwaltung finden Sie unter www.stelle.admin.ch