

DIE ZUKUNFT DER KRIMINALITÄT

EDITORIAL

**Sehr geehrte Leserin,
sehr geehrter Leser**

Wer über die Zukunft der Kriminalität nachdenkt, wird mit der Frage konfrontiert, ob kriminelles Verhalten universell oder kulturell determiniert ist. Gibt es eine spezifische Kriminalität der Zukunft oder ändern sich einfach die Umstände? Mord zum Beispiel wird in fast allen Zeiten und Gesellschaften sanktioniert. Diebstahl hingegen kann nur dann ein Delikt sein, wenn die Gesellschaft das Eigentum kennt (was inzwischen universalisiert ist, in einigen Stammesgesellschaften und politischen Ideologien aber anders war). Um die Universalität der Pädophilie als kriminellen Akt zu relativieren, muss man nicht einmal in die Antike zurückschauen. Ein Blick ins 19. Jahrhundert nach England genügt: Dort betrug das Schutzalter für Mädchen 13 Jahre. Welches Verhalten deviant ist, ist eine Frage des Wertesystems. Die Legende von Robin Hood lehrt, dass die moralische Frage nach Täter und Opfer nicht immer eindeutig ist.

Es ist erstaunlich, wie viele Science-fiction-Filme einfach unsere Vorstellungen der Kriminalität in die Zukunft projizieren, neue Spielarten der Delinquenz tauchen aber selten auf. Waffen und Transportmittel sind futuristisch – oder geradezu archaisch magisch. Der Kampf des Guten gegen das Böse wird im Cyberspace oder im Weltall geführt, Täter und Diebesbeute sind extraterrestrisch, die Delikte aber bleiben meistens identisch – wie übrigens auch die Motive und die sozialen Typen der Täter.

Wir denken in diesem Swissfuture-Bulletin über neue Tätertypen nach: Könnten aufgrund des soziodemografischen Wandels und Wohlstandsabbaus Senioren als neue Tätergruppe auftauchen? Welches werden zukünftige Motive der Täter sein? Handeln sie rational, wie es der Autor Valentin Landmann vertritt? Lässt sich das Problem also zukünftig über Anreize lösen? Oder hat der Täter eine neurologische Prädisposition, wie es der Forensiker Hans Markowitsch in seinem Beitrag darstellt?

Die soziale Mobilität nimmt zu. Neue Technologien werden neue Formen der Kommunikation und Organisation ermöglichen. Die Kriminalität wird zum globalen Phänomen mit beträchtlicher ökonomischer Wertschöpfung. Trotzdem wird kriminelles Verhalten noch immer im nationalstaatlichen Rahmen sanktioniert. Der Autor Marc Henauer bezweifelt, dass die Trennung zwischen virtueller und realer Welt kriminologisch noch Sinn macht.

Unsere Suche nach Autoren hat uns gezeigt, dass wir erst am Anfang der Fragen nach der Kriminalität der Zukunft stehen. Police Futurists International oder der Schweizerische Polizeiiformatikkongress thematisieren, dass neue, zukunftsorientierte Konzepte innerer Sicherheit nötig werden – wir sind neugierig, wie die Zukunft aussehen wird.

Dr. Andreas M. Walker und Francis Müller

FÜHRT DER MEGATREND LANGLEBIGKEIT ZU EINER NEUEN ALTERSKRIMINALITÄT?

Wenn die Lebenserwartung linear zunimmt, dürfte sie in den Industrieländern im Jahr 2060 bei hundert Jahren liegen. Dies wird weit reichende soziale Folgen haben. Wird es im Zuge des Abbaus von Sozialleistungen und der damit verbundenen Altersarmut zu einem Anstieg der Alterskriminalität kommen? Einige Indikatoren sprechen dafür.

Dr. Andreas M. Walker

Während der vergangenen Jahrhunderte betrug die Lebenserwartung zwischen 35 bis 40 Jahre. Seit 160 Jahren stieg die Lebenserwartung und nahm in erstaunlich kontinuierlichem Masse pro Jahr um drei Monate zu – insgesamt um knapp 40 Jahre. In etwas mehr als einem Jahrhundert hat sich die Lebenserwartung sowohl für Männer als auch für Frauen nahezu verdoppelt. Der Bestand an 65-jährigen und älteren Personen hat sich in der Schweiz innerhalb von 100 Jahren um das Sechsfache erhöht.

Voraussagen über eine vermeintliche Obergrenze der Lebenserwartung haben sich immer wieder als falsch erwiesen und Studien über die Sterblichkeit im hohen Alter zeigen, dass das höchstmögliche Lebensalter noch nicht definiert ist. Wenn sich der lineare und kontinuierliche Zuwachs der Lebenserwartung fortsetzt, dann wird angenommen, dass die Lebenserwartung um 2060 in den Industrieländern hundert Jahre betragen wird. Bereits heute gibt es in Deutschland 45-mal mehr Hundertjährige als im Jahr 1960. In der Schweiz hat sich die Zahl der 100-jährigen Jubilare seit 1950 in jedem Jahrzehnt mindestens verdoppelt. Swissfuture wird sich im Jahr 2009 in einer besonderen Veranstaltungsreihe mit dem Megatrend Langlebigkeit in seinen interdisziplinären Bezügen befassen.

Demografischer Wandel

Schon bald wird in der Schweiz die über-60-jährige Bevölkerung über ein Drittel und die über-50-jährige Bevölkerung über die Hälfte

der Bevölkerung ausmachen. Seit 1910 steigt der Anteil der Älteren kontinuierlich, während jener der Jungen schwindet, so dass heute mehr über-60-jährige Senioren als unter-20-jährige Junioren in der Schweiz leben. Die Zahl der Rentnerinnen und Rentner je 100 Personen im erwerbsfähigen Alter steigt bis 2050 auf 51; dies entspricht einem Verhältnis von 1:2. Allmählich wächst das Bewusstsein, dass die demografische Alterung nicht nur die Altersstruktur der Bevölkerung nachhaltig verändert, sondern auch weit reichende gesellschaftliche Folgen haben wird.

Senioren als Opfer – Senioren als Täter? Dass in unserer Gesellschaft Seniorinnen und Senioren bevorzugt zu Opfern von Verbrechen werden, ist mittlerweile allgemein bekannt und wird in Medien und Politik häufig und gerne aufgegriffen. Ob diese Vermutungen tatsächlich zutreffen, kann leider statistisch nicht verifiziert werden, da die publizierten Opferhilfestatistiken in der Schweiz nur die drei Alterskategorien «<18 Jahre», «18-29 Jahre» und «>30 Jahre» unterscheiden. Es ist jedoch nahe liegend, dass Senioren als Zielgruppe für Verbrechen attraktiv sind:

- Senioren sind in den letzten Jahren deutlich wohlhabender geworden.
- Senioren sind immer weniger in ein soziales, familiäres Umfeld integriert. Die allgemeine Verbreitung von Kleinhaushalten widerspiegelt die aktuelle Tendenz, im Rentenalter zu zweit und im

Hochbetagtenalter in der Regel alleine zu wohnen. Gemeinsam mit anderen Personen einen Haushalt zu führen wird mit zunehmendem Alter immer unwahrscheinlicher.

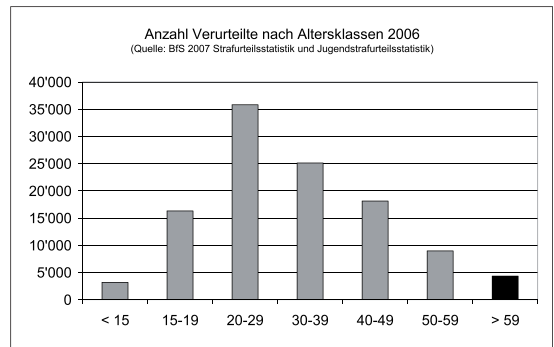
Entsprechend werden diese Zielgruppe und ihre Problematik aufgrund ihrer Kaufkraft für die Sicherheitsindustrie und aufgrund der demografisch wachsenden Macht für die Politik immer interessanter.

Werden Senioren auch zunehmend zur Täterschaft?

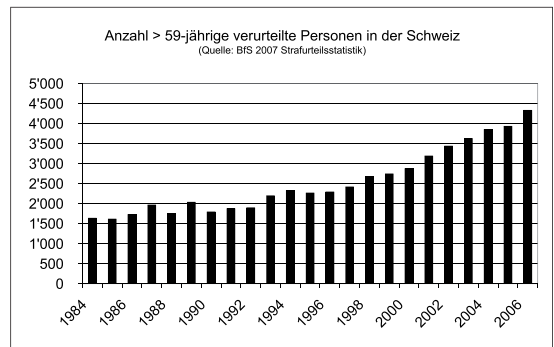
Sowohl Filmindustrie wie auch Boulevard- und Unterhaltungsmedien greifen dieses Thema gerne auf. Kriminelle im Seniorenalter sind kein Einzelfall mehr und werden mit grosser Medienbeachtung thematisiert. So erbeutete in Nordrhein-Westfalen ein Gangster-Trio aus drei Herren im Alter von 63, 72 und 74 Jahren bei mehreren Banküberfällen insgesamt 400'000 Euro – bewaffnet mit Pistolen, Handgranaten und Vorschlaghämmern. Und in Fort Lauderdale wurde ein 96-jähriger Mafioso wegen Raubes, Geldwäscherei und Bankbetrug verurteilt. Er starb beim Verlassen des Gerichtssaales eines natürlichen Todes.

Ein Blick in die Statistik zeigt, dass diese spekulative Annahme tatsächlich nachgewiesen werden kann. Das Statistische Bundesamt Deutschland meldet, dass die Zahl der kriminellen Rentner in den vergangenen 10 Jahren um knapp 30% gestiegen ist. In der Schweiz ist die Alterskriminalität in den Jahren 1984 bis 2004 um 131% bei einer durchschnittlichen Zunahme von 69% gestiegen. Innert zweier Jahrzehnte hat sich die Zahl der über 60-jährigen Männer im Strafvollzug fast verdoppelt. 1984 wurden 1'638 über 60-jährige Männer verurteilt, 2004 waren es 3'791.

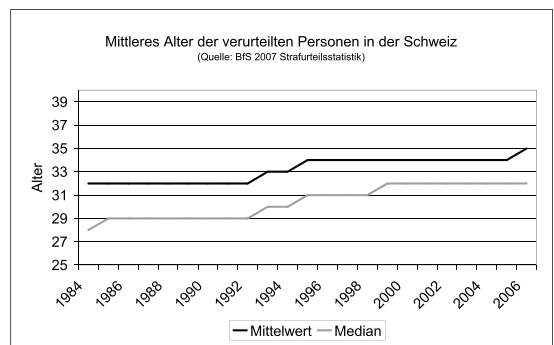
Zwar ist die Altersklasse der Senioren immer noch eine kleine Gruppe:



Aber deren absolute Zahl ist am Steigen:



Dies wirkt sich auch auf das mittlere Alter der verurteilten Personen aus:

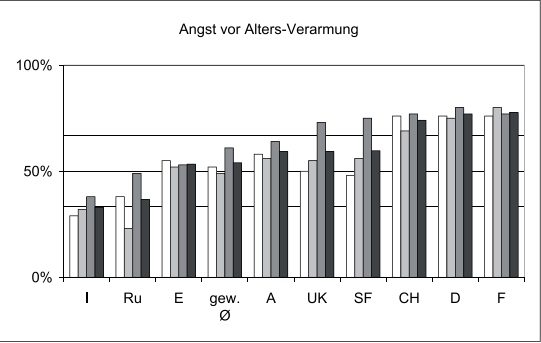


Aufgrund der demografischen Entwicklung ist die absolute und relative Zunahme der älteren Täterschaft eigentlich naheliegend.

Neuer Megatrend «Altersarmut» als Grundlage für neue Alterskriminalität?

In der Meinungsumfrage der Stiftung für Zukunftsfragen zu Europa 2030 wurden drei Fragen gestellt, die zu einer Angst-vor-Alters-Verarmungs-Quote kombiniert werden können:

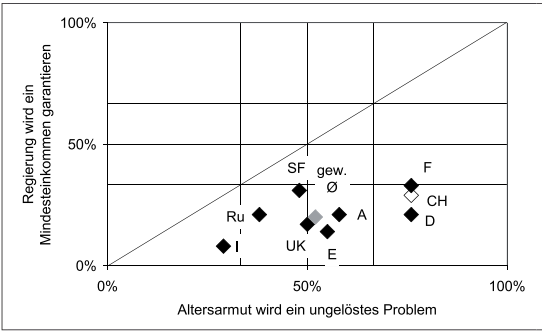
- Altersarmut wird ein ungelöstes Problem sein.
 - Viele Angestellte werden nicht genug verdienen um für die Pensionierung zu sparen.
 - Produkte des täglichen Gebrauchs (Lebensmittel) werden deutlich teurer werden.
- ➔ **Angst-vor-Alters-Verarmungs-Quote**



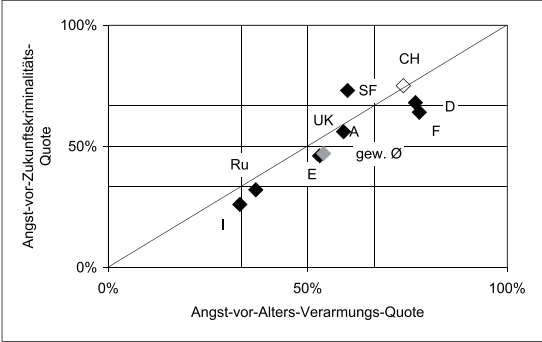
Bei allen drei Fragen und auch in der gemittelten Quote befindet sich die Schweiz jeweils in der Spitzengruppe mit einem Anteil von über 2/3 der Befragten. Auffällig ist, dass in Süd- und Osteuropa diese Angst am wenigsten verbreitet ist.

Falls sich also langfristig nicht die Megatrends «Langlebigkeit x Alterswohlstand» sondern «Langlebigkeit x Altersarmut» überlagern sollten, würden nicht nur neue, soziale Probleme sondern auch eine potenzielle neue Quelle von Kriminalität auftauchen.

Die Meinungsumfrage der Stiftung für Zukunftsfragen zu Europa 2030 lässt annehmen, dass die Angst vor Altersarmut relativ viel grösser ist als das Vertrauen auf die Regierung, dass diese dieses Problem finanziell lösen kann. Die mitteleuropäischen Länder bilden dabei die Spitzengruppe:



Auffällig ist die Korrelation der «Angst-vor-Altersverarmung» und der «Angst-vor-Zukunftskriminalität». Zeigt sie einfach auf, wie wenig differenziert die Befragten in der Wahrnehmung ihrer eigenen Ängste und in der Formulierung düsterer Zukunftsbilder sind? Oder drückt sich dabei unterschwellig auch eine unerwartete Bereitschaft aus, dass bei einer Verarmung im Alter ohne Hilfe der Regierung die Bereitschaft steigen wird, seinen eigenen Lebensunterhalt auch mit illegalen Mitteln zu sichern?

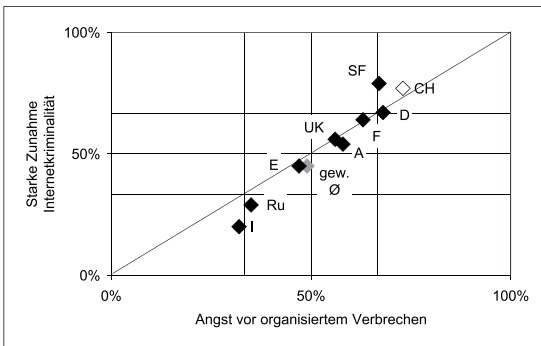


So nennt Prof. Dr. Hardtung als Ursachen für die Zunahme der Senioren-Kriminalität neben dem demografischen Faktor auch die wachsende Altersarmut und das Gefühl der Perspektivlosigkeit. Werden Verarmung und Vereinsamung tatsächlich wichtige Ursachen der Seniorenkriminalität werden? Als der Autor dieses Aufsatzes aufgrund seines Referates am Schweizerischen Polizeiformatikkongress SPIK eine unerwartete Medienresonanz auslöste, eröffneten ihm diverse Seniorinnen im persönlichen Gespräch, dass sie unlängst auch schon Ladendiebstahl verübt hätten – aus Langeweile und Nervenkitzel.

Welche Form von Kriminalität?

Spätestens hier taucht die Frage nach der Form der Kriminalität auf. Die Statistiken zeigen, dass nach wie vor besonders häufig junge Männer straffällig werden, insbesondere, was schwere Verbrechen angeht. Dies wird auch durch die Aggressions- und Gewaltforschung betätigt. Gegen Senioren als Tatverdächtige wird meistens wegen Diebstahl, insbesondere Ladendiebstahl, Betrug, Trickgaunerei und Erpressung ermittelt. Je nach zitierten Statistiken sind auch die Strassenverkehrsunfälle der Senioren gesondert zu betrachten. Die Meinungs-umfrage der Stiftung für Zukunftsfragen zu Europa 2030 geht jedoch das Thema der Kriminalität der Zukunft über zwei Indikatoren an:

- Organisiertes Verbrechen wird in allen europäischen Ländern ein grosses Problem sein.
- Internetkriminalität wird stark zunehmen.



Die heute hoch entwickelten und wohlhabenden mitteleuropäischen Länder und insbesondere die Schweiz weisen dabei Spitzenwerte aus. Italien und Russland, die in der allgemeinen Wahrnehmung als Mutterländer der mafiösen Kriminalität gelten, weisen erstaunlicherweise die geringsten Werte auf.

Sowohl in der stark arbeitsteiligen organisierten Kriminalität, die geradezu als eigene Wirtschaftsbranche betrachtet werden kann, wie auch in der Internetkriminalität spielen körperliche Kraft, Aggressionsbereitschaft

und junges Alter aber immer weniger eine Rolle. Im Hinblick auf die Kriminalität der Zukunft muss berücksichtigt werden, dass wir selbst die Senioren des zukünftigen Zeithorizontes sein werden:

- wir sind technisch kompetent
- wir sind gut vernetzt
- wir sind zunehmend «globalisiert» und multikulturell.

Dies kann bedeuten, dass organisiertes Verbrechen und Internetkriminalität nicht nur unsere Zukunftsängste widerspiegelt, sondern dass unsere Generation die skills mitbringt, um in dieser Branche erfolgreich zu sein. Damit taucht die Frage auf, ob die Umfrage zu 2030 nur die Angst vor Formen der Zukunftskriminalität ausdrückt oder eben gerade auch die Akzeptanz dieser Kriminalitätsformen.

Die kritischen Fragen an uns und an unsere Zukunft lauten also:

- Wird zukünftige Altersarmut dazu führen, dass Senioren als zunehmend wachsende Bevölkerungsgruppe auf illegalen Wegen ihren Lebensunterhalt sicherstellen werden?
- Werden organisierte Kriminalität und Internetkriminalität aufgrund der Gewalts- und Aggressionsferne und insbesondere auch aufgrund der Arbeitsteilung und Zersplitterung der «Wertschöpfungskette» des Verbrechens zwischen Täter, Tat und Opfer dazu führen, dass die Hemmschwelle drastisch sinken wird, so dass eigene Tätigkeiten «im weiteren Umfeld der Wirtschaftsbranche Kriminalität» gar nicht mehr als kriminell empfunden werden bzw. in der eigenen moralischen Wahrnehmung bagatellisiert werden?

Quellen

Bühlmann Beat (2006) Gefängnis wird zum Altersheim, in: Tagesanzeiger Zürich, 18. April 2006

Bundesamt für Statistik (2004); Alter und Generation – Das Leben in der Schweiz ab 50 Jahren

Bundesamt für Statistik (2006) Opferhilfestatistik 2005 - Beratungsfälle, Entschädigungen und Genugtuungen

Bundesamt für Statistik (2006) Die Sterblichkeit der Schweizer Geburtsjahrgänge 1900 bis 2030; demos - Informationen aus der Demografie, Heft 2/2006

Bundesamt für Statistik (2007) Demografische Alterung und soziale Sicherheit; demos - Informationen aus der Demografie, Heft 4/2007

Bundesamt für Statistik (2007) Strafurteilsstatistik, Statistisches Lexikon der Schweiz, Stand der Datenbank: 11.10.2007

Bundesamt für Statistik (2007) Statistik der Jugendstrafurteile, Statistisches Lexikon der Schweiz, Stand der Datenbank: 15.09.2008

Bundesamt für Statistik (2008); Kriminalität und Strafrecht, Panorama Februar 2008

Fasolin Sarah (2005) Brennpunkt Strafvollzug - Sitzen je nach Altersklasse; in: Der Schweizer Beobachter; 02.09.2005; Seite 42; Nr 18

Hardtung Bernhard (2007) Alterskriminalität: Alte Menschen als Täter und Opfer; Im Rahmen der Ringvorlesung 2006/2007 der Universität Rostock: Der alternde Mensch in einer alternden Gesellschaft Chancen, Risiken und Perspektiven; n.p.

Koepke Christian (2007) Alterskriminalität nimmt zu, Schweriner Volkszeitung 10.02.2007

Max-Planck-Gesellschaft (2007) Hundert wird bald jeder, Presseinformation vom 27.09.2007

Max-Planck-Gesellschaft (2002) Immer mehr Hundertjährige, Presseinformation vom 10.05.2002

Roos, George T. (Hsg.), Reinhardt, Ulrich, Stiftung für Zukunftsfragen (2008) Future Expectations for Europe, Pan-European Futures Study with Comments, Darmstadt, ISBN: 978-3-89678-803-0

Roos, George T. (Hsg.), Reinhardt, Ulrich, Stiftung für Zukunftsfragen (2009) Wie die Europäer ihre Zukunft sehen: Antworten aus 9 Ländern, Darmstadt, ISBN: 978-3896788023

Stiftung für Zukunftsfragen (12.01.2009) Wie Europäer ihre Zukunft sehen - BAT Stiftung für Zukunftsfragen veröffentlicht neue Europastudie - „Arbeiten ohne Ende.“ „Armut ohne Grenzen.“ „Leben ohne Sicherheiten.“ In: Forschung aktuell, 211, 30. Jg.

Andreas M. Walker



Dr. Andreas M. Walker (1965, Basel, verheiratet, Vater von 4 Kindern), Vorstand swissfuture, Full Member of the Association of Professional Futurists, Eigentümer von www.weiterdenken.ch, studierte Geografie, Geschichte und Germanistik, gewann mit seiner Doktorarbeit in Wirtschaftsgeografie zu Methoden des vernetzten Denken und der Zukunftsforschung und Szenariotechnik zwei Awards, Miliz-Ausbildungsoffizier eines Armeestabsteiles, der sich mit nichtmilitärischen Krisen und Katastrophen beschäftigt, Referent am 2. Schweizerischen Polizeinformatikkongress www.spik.ch zu Crime 2.0 - Verbrechen der Zukunft



ZUKUNFTSÄNGSTE 2030 – KRIMINALITÄTSÄNGSTE 2030

Eine Studie über die Zukunftserwartungen fürs Jahr 2030 in verschiedenen europäischen Ländern zeigt ein eher düsteres Bild, das geprägt ist von Ängsten vor Verarmung und Wohlstandsabbau. Dies dürfte kriminelles Verhalten – und somit neue Ängste wachrufen.

Dr. Andreas M. Walker

Zukunftserwartungen Europa 2030

Im Sommer 2008 befragte die Gesellschaft für Konsumforschung im Auftrag der Stiftung für Zukunftsfragen in einer repräsentativen Face-to-Face-Befragung 11'100 Personen ab 14 Jahren in den neun europäischen Ländern Deutschland, Finnland, Frankreich, Grossbritannien, Italien, Österreich, Russland, Spanien und der Schweiz zu deren Zukunftserwartungen für das Jahr 2030.

Düsteres Zukunftsbild Europa 2030

Die Zukunft hat viele Gesichter, diese Befragung zu den Zukunftserwartungen 2030 der Europäerinnen und Europäer zeigt aber ein eher düsteres Bild. Im Zentrum des Zukunftsbildes 2030 stehen Zukunftsängste und Zukunftssorgen. Die Stiftung für Zukunftsfragen geht in ihrer Interpretation davon aus, dass viele Europäerinnen und Europäer nicht etwa hoffnungsvoll in die Zukunft schauen, sondern bis zum Jahr 2030 sorgenvoll eine grundlegende Wohlstandswende mit weitreichenden Folgen befürchten: Arbeiten ohne Ende, Armut ohne Grenzen und Leben ohne Sicherheiten. Es überwiegt die Angst vor sozialem Abstieg und einer unsicheren Zukunft. Der Blick in die Zukunft ist eher negativ und fast entmutigend.

Dr. Ulrich Reinhardt, geschäftsführendes Vorstandsmitglied der Stiftung für Zukunftsfragen, meint dazu: «Europas Zukunft steht am Scheideweg. Die Furcht der Bürger vor

einer zunehmenden Teilung der Gesellschaft zeigt sich überall deutlich. Viele Bürger haben Angst, am Ende zu den Verlierern zu gehören.»

Prof. Dr. Horst W. Opaschowski, der wissenschaftliche Leiter der BAT Stiftung für Zukunftsfragen: «Zukunftshoffnung können sich immer weniger Europäer leisten.» Positive Erwartungen wie eine Vollbeschäftigung durch abnehmende Bevölkerungszahlen, gleiche Bildungschancen für alle Kinder oder die Lösung von Hungersnöten werden nur von einer Minderheit der Europäer erwartet.

Fragstellungen dieses Aufsatzes

Auf der Grundlage des publizierten Datenermaterials der «Future Expectations for Europe 2030» wurde nun sondiert, ob spezifische Aussagen zur Kriminalität der Zukunft möglich sind, insbesondere ob Aussagen zu Angstvorstellungen sinnvoll mit Aussagen zu zukünftigen Kriminalitätsvorstellungen verknüpft werden können. Dabei wurden die Indikatoren untersucht, die relevant für Fragen der inneren Sicherheit und der Kriminalität sind, Indikatoren zu äusserer Sicherheit wurden vernachlässigt.

Angst vor Verarmung

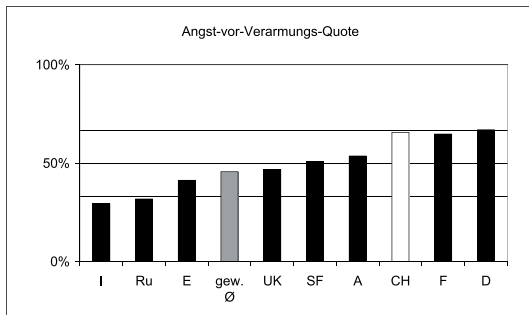
In der Meinungsumfrage zu Europa 2030 lassen sich verschiedene Indikatoren zu einer «Angst-vor-Verarmungs-Quote» zusammenfassen:

- Die Regierung wird (k)ein Mindesteinkommen garantieren
- unabhängig von Alter, Geschlecht, Herkunft, etc.
- Die Mittelklasse wird grösstenteils verschwunden sein.
Viele Angestellte werden nicht genug verdienen,
um für die Pensionierung zu sparen.
- Altersarmut wird ein ungelöstes Problem sein.
- Die Kluft zwischen arm und reich wird grösser werden.
Produkte des täglichen Gebrauchs (Lebensmittel) werden
deutlich teurer werden.

➡ **Angst-vor-Verarmungs-Quote**

Eindrücklich ist die starke Angst vor zukünftiger materieller und finanzieller Verarmung, was einige provozierende Fragen herausfordert:

- Wird die Verarmungsangst die Hemmschwelle zur Kriminalität sinken lassen?
- Wird man zukünftig vermehrt bereit sein, sich auf illegalen Wegen zu bereichern, wenn befürchtet wird, dass die legalen Möglichkeiten immer stärker schwinden?
- Wird es zukünftig überhaupt noch ökonomisch sinnvoll sein, einem bürgerlichen und geordneten Erwerbsleben nachzugehen?



Bei der Analyse dieser verdichteten «Angst-vor-Verarmungs-Quote» fällt auf, dass insbesondere in den mitteleuropäischen Ländern inklusive der Schweiz mit einem hohen Mass an sozialer und an innerer Sicherheit etwa 2/3 der Bevölkerung Angst vor einem allgemeinen sozialen Abstieg haben. In den süd- und osteuropäischen Ländern ist diese Angst bei nur etwa 1/3 der Bevölkerung wesentlich weniger relevant.

Die Mittelklasse wird grösstenteils verschwunden sein.									
Ru	SF	E	A	CH	D
18%	24%	25%	56%	68%	68%
Viele Angestellte werden nicht genug verdienen, um für die Pensionierung zu sparen.									
Ru	I	gew.	CH	D	F
23%	32%	49%	69%	75%	80%
Altersarmut wird ein ungelöstes Problem sein.									
I	Ru	SF	F	CH	D
29%	38%	48%	76%	76%	76%
Die Kluft zwischen arm und reich wird grösser werden.									
I	Ru	E	F	CH	D
39%	42%	49%	75%	75%	82%
Produkte des täglichen Gebrauchs (Lebensmittel) werden deutlich teurer werden									
I	Ru	E	CH	F	D
38%	49%	53%	77%	77%	80%
Die Regierung wird ein Mindesteinkommen garantieren unabhängig von Alter, Geschlecht, Herkunft, etc.									
F	SF	CH	UK	E	I
33%	31%	29%	17%	14%	8%
"Angst-vor-Verarmungs-Quote"									
I	Ru	E	F	CH	D
34%	34%	47%	71%	73%	76%

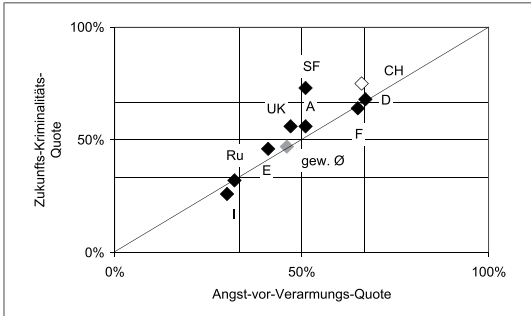
Auch die Detailanalyse dieser «Verarmungs-Ängste» zeigt,

- dass die Schweiz immer in der Spitzengruppe der zukünftigen Verarmungsängste liegt,
- dass mit Ausnahme der Frage nach der Existenzsicherung durch die Regierung immer die drei Länder Schweiz, Deutschland und Frankreich diese Spitzengruppe bilden, bei der zu jedem Indikator 1/3 der Befragten entsprechende Verarmungsängste äusserte,
- dass Italien, Russland und Spanien immer am anderen Ende der Skala liegen und am wenigsten Verarmungsängste aufweisen.

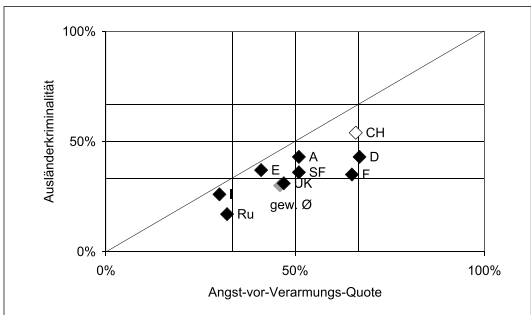
Angst vor zukünftiger Verarmung und Angst vor zukünftiger Kriminalität

Zwischen den Befragungsergebnissen der Angst vor Verarmung und denen der Angst vor Kriminalität lässt sich nun tatsächlich eine Korrelation feststellen – mit Ausnahme von Finnland (SF). Bemerkenswert ist, dass

die beiden «Mutterländer» der organisierten Kriminalität – Italien und Russland – auffällig geringe Werte aufweisen. Aufgrund der Umfrage kann nur spekuliert werden: Ist hier die organisierte Kriminalität bereits derart präsent, dass gar keine weitere Zunahme befürchtet wird? Oder wird sie hier etwa gar nicht als Problem empfunden?



Bedeutet dies nun, dass in den heute wohlhabenden mitteleuropäischen Ländern eine Kriminalität stark steigen wird, die sowohl organisiert wie auch einheimisch ist? Die nachfolgende Analyse dieser beiden Fragestellungen widerspricht eigentlich dieser Annahme. Das Resultat ist aber merkwürdig und wirft die Frage auf, ob dies tatsächlich ein stichhaltiger Indikator ist, oder ob es viel mehr darauf hindeutet, dass die beiden Fragen nach einer zukünftigen Zunahme der Verarmung und nach einer zukünftigen Zunahme der Ausländerkriminalität gegenüber der Einheimischenkriminalität primär unreflektierte Ängste wiedergibt. Die Schweiz bildet in dieser Ängste-Kombination den Spitzenwert.



Welches werden nun die richtigen Szenarien für zukunftsorientierte Kriminalitätsforschung sein?

- Wenn in den reichen mitteleuropäischen Ländern die Verarmung zunehmen wird – wird dann in diesen Ländern die endogene Kriminalität zunehmen, da hier die Chancen für legalen finanziellen Erfolg immer kleiner werden?
- Wird dies bedeuten, dass diese Länder weniger Zielländer des Verbrechens werden?
- Werden diese Länder vielleicht sogar neue Quellländer des organisierten internationalen Verbrechens werden?
- Wird in einer zunehmend globalisierten Welt, in der durch Mobilität und Virtualität die räumlichen Distanzen immer weniger eine Rolle spielen werden, die Frage nach der Nationalität der Verbrecher überhaupt noch eine relevante Frage sein?

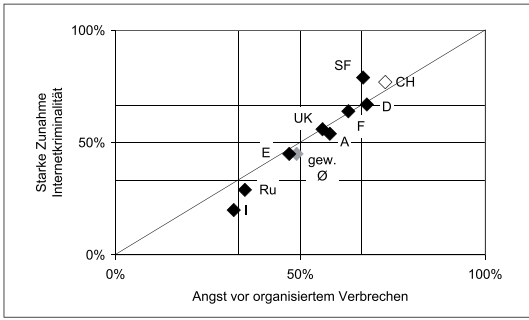
Welche Kriminalität der Zukunft?

Leider wurde in der Umfrage zu Europa 2030 nicht danach gefragt, ob die Bevölkerung überhaupt eine Zunahme der Kriminalitätsrate befürchtet. Auch wurde keine Frage nach der Bedeutung der «konventionellen Kriminalität» gestellt. Dafür wurde konkret nach organisiertem Verbrechen und Internetkriminalität gefragt.

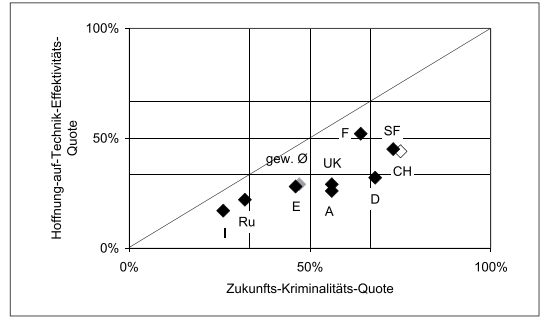
- Organisiertes Verbrechen wird in allen europäischen Ländern ein grosses Problem sein.
 - Internetkriminalität wird stark zugenommen haben.
- ➡ **Zukunfts-Kriminalitäts-Quote**

Die Analyse der Umfragewerte zeigt, dass diese beiden Werte zu korrelieren scheinen, wobei die Angst vor Internetkriminalität in Italien und Russland relativ geringer und in Finnland relativ grösser ist. Die Schweiz bildet wieder den Spitzenwert mit der höchsten Sensibilität für beide Themen, Italien und Russland das Schlusslicht, obwohl gerade Russland in der öffentlichen

Wahrnehmung gerne als Quellland von organisierter Kriminalität und von Internetkriminalität betrachtet wird.



Dabei lassen sich folgende Meinungen bzw. Ängste feststellen:



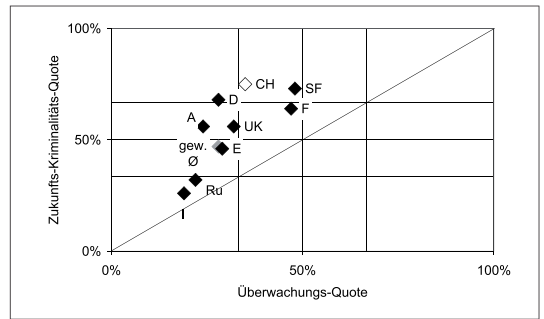
High Tech als Hilfe gegen zukünftige Kriminalität

Technischer Fortschritt, Globalisierung und weltumspannende Kommunikation werden allen Seiten zu Gute kommen – werden nun Kriminelle oder Polizei im technologischen Wettrüsten der Zukunft die Oberhand haben?

Zur Annäherung an die Meinungen zu dieser Fragestellung wurden wiederum verschiedene der Indikatoren der Studie zu Europa 2030 einzeln bzw. verdichtet ausgewertet:

- Europäischer/internationaler Datenaustausch wird helfen, Verbrechen schneller aufzuklären, die Bevölkerung wird sich sicherer fühlen als heute.
 - Viele Leute werden zur Identifikation und Lokalisation einen Chip tragen
 - Für viele Personen wird Sicherheit wichtiger sein als ihre Privatsphäre.
 - Überwachungscomputer werden zahlreiche Kriminelle direkt bei Begehen der Tat identifizieren.
- ➡ **Hoffnung-auf-Technik-Effektivitäts-Quote**

➡ Die Angst vor Zukunfts-Kriminalität ist grösser als die Hoffnung auf eine effektive High-Tech-Polizei. Die Schweiz befindet sich in der Spitzengruppe.



➡ Trotz Angst vor einer Zunahme der Zukunfts-Kriminalität besteht keine Bereitschaft auf einen Verzicht auf Datenschutz und Privatsphäre.

- Viele Leute werden zur Identifikation und Lokalisation einen Chip tragen.
 - Für viele Personen wird Sicherheit wichtiger sein als ihre Privatsphäre.
- ➡ **Überwachungs-Quote**

Weiterführende Fragen

Die von der Stiftung für Zukunftsfragen durchgeführte Meinungsumfrage zu Europa 2030 liefert vielfältiges Datenmaterial. Auf dieser Grundlage stehen aber nun einige interessante Problembereiche zur Vertiefung an:

- Sind die konstanten Höchstwerte der Schweiz und die konstanten Tiefstwerte von Italien und Russland tatsächlich fachlich begründet oder spiegeln sie einfach Ängste und Sensibilitäten der Bevölkerung wieder, die sich primär dadurch begründen, dass die Schweiz besonders viel und Italien und Russland eher wenig zu verlieren haben?
- Falls es tatsächlich zu sozialen Verschiebungen in den verschiedenen europäischen Ländern und zu einem starken Anwachsen einer neuen Unterschicht in Mitteleuropa kommen wird, wird dies zu neuen Quell- und Zielländern der organisierten Kriminalität führen?
- Werden die Ängste aus der repräsentativen Meinungsumfrage in der Bevölkerung auch von Experten aus Kriminalitätsforschung und Fachleuten aus der Polizei bestätigt?
- Beurteilen eben diese die Chancen einer High-Tech-Polizei gegenüber den High-Tech-Kriminellen ebenfalls derart kritisch?



Andreas M. Walker



Dr. Andreas M. Walker (1965, Basel, verheiratet, Vater von 4 Kindern), Vorstand swissfuture, Full Member of the Association of Professional Futurists, Eigentümer von www.weiterdenken.ch, studierte Geografie, Geschichte und Germanistik, gewann mit seiner Doktorarbeit in Wirtschaftsgeografie zu Methoden des vernetzten Denken und der Zukunftsforschung und Szenariotechnik zwei Awards, Miliz-Ausbildungsoffizier eines Armeestabsteiles, der sich mit nichtmilitärischen Krisen und Katastrophen beschäftigt, Referent am 2. Schweizerischen Polizeiiformatikkongress www.spik.ch zu Crime 2.0 - Verbrechen der Zukunft

Literatur

Roos, George T. (Hsg.), Reinhardt, Ulrich, Stiftung für Zukunftsfragen (2008) Future Expectations for Europe, Pan-European Futures Study with Comments, Darmstadt, ISBN: 978-3-89678-803-0

Roos, George T. (Hsg.), Reinhardt, Ulrich, Stiftung für Zukunftsfragen (2009) Wie die Europäer ihre Zukunft sehen: Antworten aus 9 Ländern, Darmstadt, ISBN: 978-3896788023

Stiftung für Zukunftsfragen (12.01.2009) Wie Europäer ihre Zukunft sehen - BAT Stiftung für Zukunftsfragen veröffentlicht neue Europastudie - „Arbeiten ohne Ende.“ „Armut ohne Grenzen.“ „Leben ohne Sicherheiten.“ In: Forschung aktuell, 211, 30. Jg.,

ÖFFENTLICHE SICHERHEIT IM INTERNET WAHREN

Das Internet eröffnet Chancen, aber auch Gefahren. 84% der 14- bis 29-Jährigen nutzen das Internet regelmässig – und kommen dabei auch sehr schnell in virtuellen Kontakt mit pädophil veranlagten Sexualstraftätern. Die Staatsaufgabe der öffentlichen Sicherheit muss auch in der digitalen Welt standhalten.

Barbara Schmid-Federer, Nationalrätin

Claudio F., 34, wird zunehmend beherrscht durch unverhältnismässige sexuelle Phantasien. Unverhältnismässig deshalb, weil er dabei auch an Gewalt denkt: Er verspürt Lust, jungen Mädchen Schmerzen zuzufügen. Claudio F. ist eigentlich ein schüchterner Mensch. Im realen Leben getraut er sich nicht, sich einem Mädchen zu nähern, an Freundschaften mit jungen Girls ist nicht zu denken. Regelmässig konsumiert er Pornografie im Internet. Je länger je brutalere Szenen: Inzest, Sodomie oder Pädophilie sind per Mausclick sofort zu haben.

Um nicht zu vereinsamen, loggt sich Claudio in Chatrooms ein. Unter einem Pseudonym – etwa Julia, 13 – tauscht er mit seinen Chat-»Freundinnen« intime Bilder aus. «Freundinnen», von denen er weiss, dass sie sich auf derlei Austausch einlassen, spricht er unter einem männlichen Pseudonym an – etwa Mario, 15. Mario hat «Erfolg». Regelmässig gelingt es ihm, sich die Intimbereiche junger Girls per Webcam anzuschauen. Heute ist der schüchterne Claudio F. ein erfahrener Täter. Einmal hat er eine Chatpartnerin sogar real getroffen: Sie haben sich verabredet und er konnte real versuchen, sich an ihr zu vergehen. Der schüchterne Claudio F. wäre vor 30 Jahren vielleicht schüchtern geblieben. Er hätte keine Möglichkeit gehabt, seine unverhältnismässigen Fantasien per Internet auszuleben. Und wie sieht der Claudio F. der Zukunft aus?

Vernetzt – und verletzlich

Wir leben in einer Welt, die an sich wundervoll sein könnte. Die Technologie – gerade die Informatik – bringt uns unaufhaltsam Fortschritte, die wir geniessen sollen und dürfen.

Derweil sich beispielsweise eine Wirtschaftskrise grössten Ausmasses aufbaut, bietet das Internet viele neue, zusätzliche Chancen, sich im Umbruch weiterzuentwickeln. Entsprechend boomen Online-Businessnetzwerke. Portale wie LinkedIn und Xing verzeichneten in den vergangenen Monaten aufgrund der unsicheren Joblage deutliche Nutzer- und Aktivitätszuwächse¹. Nur: Solche Social Networks sind ein ideales Einfallstor für Social Engineering. Gemäss Wikipedia handelt es sich dabei um „zwischenmenschliche Beeinflussungen mit dem Ziel, unberechtigt an Daten oder Dinge zu gelangen“. Die Tücken davon kennen wir bestens – was einmal im Netz ist, wird nie wieder verschwinden. Was einmal ein lustiges oder unüberlegtes Bilddokument war, wird später ein potenziell karrierehemmendes Problem. Dass virtuelle Welten eine seltsame Eigendynamik entwickeln können, illustrierte vor wenigen Monaten die Schlagzeile: «Virtueller Mord führt auch in den Knast – Online-Rosenkrieg hat Nachspiel im realen Leben»². Der Vorwurf, den die reale Justiz an die Täterin erhebt, ist nicht der virtuelle Mord, ausgeübt durch eine – stets in der virtuellen Welt - enttäuschte Liebende. Nein, der Vorwurf der Justiz besteht darin, dass die Frau sich unberechtigterweise Zugang zum Account des Ex-Online-Partners beschafft

hat. So gelang es ihr, den Avatar, also ein künstliches Ich des Onlinepartners (der 1'000 km weit weg lebt), zu löschen. Laut japanischem Recht drohen im Fall einer Verurteilung bis zu fünf Jahre Gefängnis oder eine Geldstrafe von 5'000 Dollar. So schnell kann es gehen, und das virtuelle Spiel wird zum Thema für die Polizei.

Was ist im Cyberspace eigentlich statthaft?

Man mag darüber denken, was man will – wir stehen vor einer grundsätzlichen Frage: Was ist im Cyberspace eigentlich statthaft? Alles, was keinen realen Schaden anrichtet? Was aber ist realer Schaden? Heisst real «materiell»? Was ist mit seelischen Schäden? Gelten im Cyberspace Werte? Und wenn ja: welche? Die Väter des Internets hatten einen Raum des freien Austauschs vor Augen. Informationen sollten frei zugänglich sein, allen staatlichen Autoritäten sei zu misstrauen. Gründervater John Gilmore erklärte: «The Net interprets censorship as damage and routes around it»³. Und Ende letzten Jahres haben sich die Internetriesen Google, Yahoo und Microsoft zu einer Initiative zum Schutz der Online-Meinungsfreiheit zusammengeschlossen, gemeinsam mit Human Rights Watch. Selbstverpflichtende Richtlinien sollen den Nutzern mehr Privatsphäre und freie Meinungsäußerung im Netz garantieren⁴. Gründervater John Gilmore hatte sich eines nicht vorstellen können: Menschen wie Claudio F..

Pornografie in Chaträumen

Dennoch: Das Internet ist aus unserem Alltag nicht mehr wegzudenken, und die jüngsten Zahlen sind eindrücklich: 84% der 14- bis 29-Jährigen nutzen das Internet regelmässig, ebenso wie immerhin 41% der Personen ab 50 Jahren. In der Summe sitzen 64% der Schweizer Bevölkerung ab 14 Jahren regelmässig vor dem Internet, also täglich oder mehrmals pro Woche.⁵ Aber: 70'000 Menschen in der Schweiz sind internetsüchtig. Das heisst: Sie verbringen mehr als 35 Stunden pro Woche privat im Netz. 35

Stunden – das ist fast das Wochenarbeitspensum. Es wird privat aufgewendet für Games, Chat und Pornografie⁶. Der durchschnittliche Schweizer Internetnutzer verbringt demgegenüber zehn mal weniger Zeit (3,5 Stunden pro Tag) im Internet⁷.

Kids benutzen den Chatraum als Kommunikationsmittel. Was jedoch kaum jemand weiss: Im durchschnittlichen Alter von 11 Jahren kommt ein Jugendlicher per Chatraum mit Pornografie in Kontakt. 89% sämtlicher Jugendlicher werden in Chaträumen sexuell belästigt. Täter sind Männer wie Claudio F.. Meist männlich, aus allen sozialen Schichten, aus sämtlichen Berufsgattungen, ca. 30 bis 45 Prozent sind unter 18 Jahre alt⁸. Während Kinder vor 30 Jahren – oft heimlich – die Zeitschrift Bravo konsumierten, wird heutigen Kindern im Internet die Frage gestellt: «Bisch no Jungfrau?» oder «Häsch Sex gern?»

Erinnern wir uns an den Fall eines 26-Jährigen Tessiners, der sich nach einem Chat nach Zürich aufmachte, um Sex mit einer 13-Jährigen zu haben: Das vermeintliche Mädchen war jedoch ein Polizist, früheren Verkehr mit einer Dreizehnjährigen hatte der Mann im Chat schon «gestanden», auf seiner Harddisk war Kinderpornographie – und das Bundesgericht sprach ihn am 16. Juni 2008 frei. Letztlich wegen Verfahrensfehlern und Unklarheiten in der Gesetzgebung. Verschiedene Polizeikorps haben das Urteil analysiert und die Konsequenzen daraus gezogen – es enthielt eine Anleitung, wie vorzugehen sei, dass man hinterher nicht in ein Beweisverwertungsverbot tappe.

In einer Motion habe ich im Frühling 2008 den Bundesrat aufgefordert, die gesamte Problematik des Chattens, inklusive Strafverfolgung, als Gesamtpaket zu beurteilen und Massnahmen zu ergreifen. In einer anderen Motion verlangte ich im Winter 2008, dass verdeckte Ermittlung im Cyberspace auch im Vorfeld von Straftaten möglich bleiben soll. Die Motivation dazu erhielt ich durch konkrete, schockierende Erlebnisse, die ich in Zusammenhang mit Chaträumen erfahren

habe. Ich habe einen Selbstversuch gemacht und mir ein Pseudonym zugelegt. Als Daniela, 13, habe ich mich in einen Chat eingeloggt. Nach 43 Sekunden wollte ein zwanzig Jahre älterer Mann Sex mit mir haben. Er hinterliess seine Email-Adresse zwecks Kontaktaufnahme, was ich natürlich bleiben liess. Andere waren hartnäckiger. Ein 36-Jähriger Mann erklärte mir als vermeintlich 13-Jährigem Mädchen, wie er gerade aus der Dusche komme und eine Webcam hätte. Das war nach 10 Minuten.

Kurzum: Für Claudio F. gibt es nichts einfacheres als das Internet. Dort kann er unbeobachtet seine Opfer aussuchen und sich mit ihnen treffen. Damit sich die meisten jungen Opfer schützen können, müssen sie entsprechend informiert werden. Aber wer soll sie informieren? Ein Grossteil der Lehrerschaft und Eltern ist in einer Zeit ohne Internet aufgewachsen: Sie haben die Entwicklungen des einzigen globalen Mediums verpasst. Fortbildungen für Pädagogen/-innen, sozialen Einrichtungen und Eltern werden in Zukunft unabdingbar sein, unabhängig von politischen Ideologien eines Staates. Je früher die Information beginnt, umso eher ist die Jugend der Zukunft vor der neuen Internetkriminalität geschützt.

Science Fiction der Zukunft: Social Fiction

Science Fiction ist das Gedankenspiel, mit neuen, unvorstellbaren technischen Möglichkeiten eine irrealer Welt aufzubauen. Allein – die Realität der IT galoppiert den Science Fiction-Szenarien davon. Zwar können wir unsere Körper noch nicht an einen anderen Ort beamten wie in «Raumschiff Enterprise», doch wird dieser Wunsch indirekt durch das Internet – den Cyberspace – erfüllt. Claudio F. kann dank technischer Mittel junge Mädchen, die er sich sonst kaum anzusprechen getraute, in Echtzeit drangsalieren – bis hin zum sexuellen Übergriff, der virtuell erfolgt, aber sehr real schadet. Es ist nur eine Frage der Zeit, bis er nebst Seh- und Hörorgan auch

das das Riechorgan dazu benutzen wird. Politisch und gesellschaftlich muss den Schattenseiten des innovativen Sturm und Drang von Science Fiction und IT etwas gegenübergestellt werden – nennen wir es Social Fiction: Die Menschen müssen wieder lernen, Freundschaften und zwischenmenschliche Gefühle real zu spüren und zu benutzen und von der IT-Welt zu trennen. Auch Claudio F. muss lernen, mit realen Menschen zu leben. Wir tragen eine Verantwortung, ihm beim Weg aus dem IT-Verkehr zu helfen – und sei es «nur» zum Schutze unserer Kinder. Er muss konkret daran gehindert werden, Jugendliche im Internet zu belästigen.

Dieser vielleicht etwas sperrigen Verantwortung kann sich kein Akteur der Gesellschaft entziehen: Grundsätzlich begrüsse ich zwar die Idee der Gründerväter, mit dem Internet einen möglichst freien, unzensierten Kommunikationsraum zu schaffen, der die Welt zusammenbringt und Raum für eine freie Entwicklung lässt. Leider aber wird – wie es ein Naturgesetz zu sein scheint – auch im Internet diese Freiheit sofort ausgenützt und zu kriminellen Zwecken missbraucht. Da das Internet eine globale Angelegenheit ist, sollte dieses Problem auch global angegangen werden und zwar im Idealfall in einem Verbund von Politik, Justiz und allen weiteren involvierten Kreisen wie Industrie, Interessengruppen, usw. Selbstverständlich ist es auch die Pflicht jedes einzelnen Rechtsstaats und damit auch der Schweiz, in Anlehnung oder Ergänzung zu den globalen Richtlinien, eigene Regeln für das Internet festzulegen und diese durchzusetzen. Mit Blick auf die Praxis heisst das für die Schweiz: Es gibt eine Verantwortung der Polizei, über die aktuelle Lage hinaus zu denken. Welches sind aber die Mittel, die sie demnach – aus strategischer Sicht – brauchen werden? Es gibt eine Verantwortung der Industrie, über die aktuellen Geschäfte hinaus zu denken. Diese muss mögliche Missbräuche ihrer Produkte voraussehen können. Es gibt auch eine Verantwortung der Politik, indem beispielsweise jedes neue Gesetz auf Herz

und Nieren dahingehend geprüft wird, ob es dem Cyberspace wirklich gewachsen ist. Es geht darum, die Staatsaufgabe «Öffentliche Sicherheit» digital zu denken. Es gibt aber auch eine Verantwortung der Gesellschaft, jedes einzelnen Mitglieds des Souveräns. Wir Bürger können und dürfen nicht einfach alles, was heikel ist, auf Politik und Polizei abwälzen. Denn so entstünde ein Polizeistaat. Das richtige Verhalten im Internet sollte demnach in Zukunft bereits Teil der Erziehung und wohl auch der Schulbildung sein.

Claudio F. im Jahre 2200

Wenn wir diese Verantwortung nicht wahrnehmen, wird sich der Claudio F. der Zukunft vermutlich an Techniken und Mitteln ergötzen, die den meisten von uns unvorstellbar sind. Durch die laufende rasante Entwicklung von Computern und Internet wird das Leiden der Kinder noch zunehmen. Vielleicht sinkt mit schwindenden Technologiekosten sogar der Preis für diesen perversen «Kick» – was den Markt vergrössern würde. Das ist eine Horrorvision, angesichts derer wir nicht vergessen dürfen, dass schon heute Kinder für die kranke Lust Erwachsener mit dem Leben bezahlen.

Uns muss ein anderer Claudio F. vorschweben. Einer, dem Hand geboten wird, sich von seiner Internetsucht zu befreien. Einer, der lernt, reale Beziehungen zu echten Freunden aufzubauen. Zu diesem Bild gehört untrennbar auch eine aufgeklärte Gesellschaft: Claudio F. fände kaum potenzielle Opfer, wenn diese gelernt hätten, die Gefahren des Internets zu erkennen. Die jungen Mädchen (und Knaben) müssen wissen, dass sowohl im realen wie im virtuellen Leben Ehrlichkeit und Vertrauen ein hohes Gut sind, mit dem nicht leichtfertig umgegangen werden darf. Dazu gehört aber auch die Erkenntnis, dass es aufgrund der Anonymität in der virtuellen Welt einfacher ist, zu lügen und zu trügen und dass sie sich zum Selbstschutz deshalb vorsichtiger verhalten müssen. Entsprechend werden in dieser Gesellschaft auch viel weniger persönliche Daten durch Publika-

on im Netz zum kaum schützbareren «Allgemeingut» gemacht. Und wahrscheinlich braucht es eine kleine, aber sehr schlagkräftige Cyberpolizei, die neuralgische Punkte kennt und vor deren Überraschung niemand sicher ist. Damit die Claudio F.s, die es noch geben wird, der Besserung zugeführt werden.

Quellen

- 1 Nach: Presstext.ch, 29.10.2008 (<http://www.presstext.ch/pte.mc?pte=081029004>)
- 2 Presstext, 24.10.08: Virtueller Mord führt auch in den Knast (<http://www.presstext.ch/pte.mc?pte=081024017>)
- 3 Uni Trier, Strafbare Handlungen im Internet, 2000, S. 9.
- 4 Presstext, 29.10.08: IT-Riesen schließen Pakt zur Online-Meinungsfreiheit (<http://www.presstext.ch/pte.mc?pte=081029023>)
- 5 Nach: Medienmitteilung SFA, SFA-Süchtig nach Onlinespielen und Chats, 20.10.08 - 10:00 - <http://www.presseportal.ch/de/meldung/100571598>.
- 6 Schweiz. Fachstelle f. Alkohol- und andere Drogenprobleme (SFA). In: «Schweizer sind süchtig nach Games und Porno», ch, 21. Okt 2008, S. 5.
- 7 Netzticker-News vom 27.10.2008: «Schweizer verbringen immer mehr Zeit im Internet» – Gemeinsam mit dem Marktforschungsinstitut Skopos hatte Planetactive im Juli/August dieses Jahres eine Online-Panelbefragung durchgeführt.
- 8 www.schaugenau.ch

Barbara Schmid-Federer



Barbara-Schmid-Federer (geboren 1965) studierte Romanistik in Zürich, in Granada und an der Sorbonne in Paris. Sie arbeitete als Gymnasiallehrerin am Freien Gymnasium in Zürich und Paris, als Prüfungsexpertin an der Schule für angewandte Linguistik SAL in Zürich, als Assistentin des Präsidenten der ETH Zürich und Leiterin der Dual Career Advice Stelle (Präsidentialstab Professoren) der ETH Zürich. Seit 2002 arbeitet sie in der Geschäftsführung der Fraumünster-Apotheke in Zürich. Barbara Schmid-Federer ist Mitglied des Präsidiums CVP Schweiz und Nationalrätin. Weiter ist sie Mitglied der Zürcher Frauenzentrale, Vizepräsidentin der Kinderhilfe Bethlehem und Präsidentin der Schweizer Sektion der Internationalen Gesellschaft für Menschenrechte (IGFM). Sie ist verheiratet und hat zwei Kinder.

«WÄCHTER 2.0»? ODER ETWA «LEVIATHAN.COM»?

Der Mensch ist des Menschen Wolf, schrieb Hobbes. Sein Vorschlag: Die Gesellschaft muss sämtliche Macht dem Leviathan abgeben, einem Souverän, dessen höchstes Ziel der Friede ist. Was bedeutet dieses Modell in Hinblick auf die neueren virtuellen Kriege aller gegen alle, die im Web 2.0 geführt werden?

Mark A. Saxer

Öffentliche Sicherheit: Das Thema gehört zu den ältesten Knacknüssen der Menschheit. Das ist auch schlüssig – das eigene Wohl geht nahe, physisch nahe. Doch so volksnah, wie das Thema oft abgehandelt wird, wurde das nicht immer angepackt. Immerhin beschäftigte es auch einige der führenden Philosophen der Weltgeschichte. Schon im ersten Monument der politischen Philosophie ist die ordnende Macht zentral: Platon postulierte in seiner Politeia, mangelnde Mässigung der Menschen erheische die Schaffung eines Wächterstandes. Er verband ihn untrennbar mit der Gerechtigkeit, dem Ziel seines Staatsentwurfs. Das war etwa um 370 v. Chr.

Über diese Wächter gäbe es viel zu sagen – doch wir wollen ja von hier aus in die Zukunft blicken. Allerdings gilt es, spätestens im Jahre 1651 nochmals innezuhalten. Damals erschien in London ein Buch, das wohl noch lange für rote Köpfe sorgen wird: Leviathan. Sein Autor, Thomas Hobbes, hatte schon 1642 unter dem Titel De Cive (über den Bürger) schnörkellos konstatiert: «Homo homini lupus» – der Mensch ist des Menschen Wolf.

Konkurrenz, Misstrauen, Ruhmsucht

In einer Analyse, der man übertriebene Sentimentalität sicher nicht vorwerfen kann, schrieb Hobbes unter anderem: «So liegen also in der menschlichen Natur drei hauptsächliche Konfliktursachen: Erstens Konkurrenz, zweitens Misstrauen, drittens Ruhmsucht.» Daraus aber ergebe sich klar, dass die Menschen ohne ordnende Macht nur in

einem Zustande des Krieges aller gegen alle leben könnten. Der Ausweg aus der permanenten Todesfurcht: Die freiwillige Übertragung aller Macht an den Leviathan. So entsteht – grob verkürzt – im hobbesschen Gesellschafts- und Herrschaftsvertrag eine Art grosser Maschine, ein gigantischer, recht-erzwingender Artefakt – ein Monstrum auch, über das seine Schöpfer nicht mehr verfügen können, dem sie ausgeliefert sind. Der Leviathan ist die vielleicht radikalste Antwort auf die Frage nach der Rolle des Staates: Er hat Frieden zu stiften, Frieden um (fast) jeden Preis. Zugegeben: Dieses Modell ist nicht gerade eben helvetisch. Und auch sonst wurde das sperrige Opus aus fast jedem Blickwinkel verrissen – ohne je zu fallen freilich. Vor allem aber scheint es auch nicht sonderlich futuristisch.

Allein: Hobbes hat uns mehr als 350 Jahre voraus. Er hat die Staatsaufgabe «öffentliche Sicherheit» konsequent durchdacht. Der Leviathan ist einer der grossen Leuchttürme der Philosophie – ein erratischer Block vielleicht, aber ein gewaltiger. Selbst Rousseau charakterisierte den Menschen im Naturzustand kaum schmeichelhafter.

Und die Society 2.0?

Und die Zukunft? Sie wird uns – philosophisch gesehen – keine neue Ausgangslage bescheren. Beispielsweise sind die Plattformen des Web 2.0 nicht zuletzt ein Spiegel von Ruhmsucht, Konkurrenz und Misstrauen. Und dass der Mensch des Menschen Wolf ist, zeigt sich kaum deutlicher als im unermesslichen Leid kleiner Kinder, real zugefügt zum

kranken, aber... digital rasend um sich greifenden Konsum. Nur dass Wölfe so etwas niemals täten.

«Verträge ohne das Schwert sind blosser Worte» – Hobbes gilt auch in der Society 2.0. Vielleicht ist seine Maschine ja ein Denkanstoss: Grundsätzlich braucht die Gesellschaft einen neuen Gesellschaftsvertrag, der die virtuelle Welt einschliesst. Und da die virtuelle Welt nicht zuletzt Maschinen-getrieben ist, liesse sich der Leviathan vielleicht weiterspinnen: Brauchen wir etwa ein Netzwerk, das kriminelle Inhalte automatisch stoppt? Maschinell, ohne Widerspruchsmöglichkeit? Wäre es eine Idee, Rechner zu bauen, die Sender perverser Inhalte automatisch blockieren und verzeigen?

Wer weiss. Wahrscheinlich gibt es bessere Ideen. Aber auf jeden Fall sind wir heute aufgerufen, die Zukunft digital zu denken. Dort anzufangen, wo die ganz Grossen der Philosophie aufhörten, ist vermutlich eine ganz taugliche Eselsleiter.



Mark A. Saxer

Mark A. Saxer studierte Politikwissenschaft an der Universität Zürich. Heute ist er einer der Leiter des Schweizerischen Polizei Informatik Kongresses (SPIK).



KRIMINELLE, STAATEN UND GEWALTEXTREMISTEN –

Wer bedroht die kritischen Informationsinfrastrukturen wirklich?

Die Trennung zwischen Informationsstrukturen und Infrastrukturen machte sicherheitstechnisch keinen Sinn. Die virtuelle und reale Welt sind durchlässig. Dies stellt die Sicherheit von Daten vor neue Herausforderungen, denn Akteure mit krimineller Energie können diese – aufgrund ganz verschiedener Motive – missbrauchen. Der Schutz der Information ist ein grosses Zukunftsthema.

Marc Henauer

Was sind eigentlich kritische Informationsinfrastrukturen? Was unterscheidet sie von so genannten kritischen Infrastrukturen? Darüber wird schon lange gerungen – und eine Ende der Debatte ist nicht in Sicht. Während das eine Lager beispielsweise gerade mal die Internetbackbones knapp als Informationsinfrastruktur anerkennt, hätten andere gerne alles, was nicht ohne einen Computer läuft, unter diesem Begriff subsumiert. Dabei liegt die Wahrheit wie so oft irgendwo in der Mitte. Im Lichte der im Titel gestellten Frage ist es allerdings gar nicht so wichtig, was genau zu den kritischen Informationsinfrastrukturen gehört und was nicht. Viel wichtiger ist die Tatsache, dass die bis anhin in den Köpfen vieler Experten zu diesem Thema verankerte Dualität zwischen physischen und virtuellen Bedrohungen so nicht mehr stimmen kann. Informationsinfrastrukturen werden nicht mehr mit ausschliesslich Informations- und Kommunikationsmittel basierten Angriffen lahmgelegt, genauso wenig, wie physische Ziele nur mit roher Gewalt ausgehebelt werden können. Diese zunehmende Interdependenz zwischen virtueller und realer Welt ist es denn auch, was eine Antwort auf die Frage im Titel relativ einfach macht: Denn alle bedrohen die kritischen Infrastrukturen und damit auch die kritischen Informationsinfrastrukturen.

Am Anfang stehen die Daten

Wie der fast schon zu Tode gerittene Ausdruck des Informationszeitalters bereits impliziert, stehen heutzutage Informationen – oder generischer ausgedrückt Daten – am Ursprung fast jeglicher Geschäfts- oder Privattätigkeit. Dabei müssen Daten nicht nur als Bilder, Dokumente oder strukturiert gespeicherte Information verstanden werden, sondern auch als Steuerbefehle und dergleichen. Es scheint dabei relativ einleuchtend, dass unlautere Absichten im Zusammenhang mit solchen Informationen oder Daten auch auf die letzteren abzielen werden. Sei es in Form von den allseits bekannten Phishingvorfällen (das sind Versuche, über gefälschte Internet-Adressen an Nutzerdaten zu kommen) im Zusammenhang mit Auktionsportalen oder Banken, oder aber die immer wieder mal in den Medien aufblitzende staatlich oder privat verübte Spionage. Aber auch das Kontrollieren von Datenströmen wird zunehmend lukrativer. Findet sich ein Rechner, der infiziert und somit einem anderen als dem Willen des eigentlichen Benutzers untertan gemacht werden kann, so lässt sich dieser wunderbar im Rahmen eines Botnetzes verwerten, selbst wenn sich keine interessanten Informationen auf dem Computer befinden. Falls es sich dabei zufälligerweise gerade noch um die Steuereinheit einer Herzlungenmaschine oder einer Mischanlage

in einem chemischen Betrieb handelt, lassen sich noch weitere, eher unschöne Anwendungsbeispiele vorstellen.

Tatsache bleibt: Wer einmal Kontrolle über die Daten eines anderen erlangt hat, kann damit anstellen was immer er will. Sei es aus reinem Eigennutz, oder aber, um diese Informationen dann wieder gewinnbringend weiter zu verkaufen. Wobei der Käufer staatlicher, privater oder sonstiger Natur sein kann. Allerdings müssen Angreifer gar nicht immer erst einen besonders listigen Weg ersinnen, um an Informationen zu gelangen. Manchmal genügt es bereits, die eigenen, teils relativ grosszügig vergebenen Zugriffsrechte auszunützen, um in den Besitz von Informationen mit hohem pekuniärem Wert zu kommen.

Wenn IT-Security nicht mehr gleich Informationssicherung ist

Wenn sich ein Bankangestellter mit ein paar tausend Kundendatensätzen, fein säuberlich auf eine CD gespeichert, aus dem Staub machen kann und für seine (gestohlene) Datensammlung auch noch einen etwa sieben- bis achtstelligen Betrag kassiert, dann hatte wohl weder eine Malware, noch ein Leck im technischen IT-Schutzwall der Bank etwas mit dieser unschönen Angelegenheit zu tun. Vielmehr lässt sich die Frage stellen, weshalb denn ein Vermögensverwalter auf viel mehr Daten Zugriff hat als er wahrscheinlich jemals an Kunden betreut. Und weshalb er diese einfach auf eine CD brennen kann, zum leichteren Transport und zur angenehmeren Übergabe an den Auslandsnachrichtendienst eines befreundeten Staates.

Das gleiche lässt sich auch dann fragen, wenn wissenshungrige Praktikanten und Studenten uneingeschränkten Zugriff auf die letzten Forschungsergebnisse eines hochspezialisierten Pharmatech-Unternehmens haben, nur um diese Information nach ihrem Ausscheiden an den höchstbietenden Konkurrenten zu verkaufen. In solchen Fällen

ist der gute Glaube an die Verlässlichkeit und den vorbildlichen Charakter der Mitarbeiter ebenso schädlich wie die Überzeugung, dass zu viel Kontrolle und Einschränkung dem freien und effizienten Informationsaustausch schaden. Genauso, wie wenn Mitarbeiter in kritischen Positionen, sei es im vertraulichen Kundengeschäft im Dienstleistungssektor oder am Schaltpult eines Kraftwerkes, nach dem gleichen Prozess wie ein temporärer Angestellter des Hausdienstes eingestellt werden (nein, auch das letzte Beispiel ist nicht erfunden).

Sie alle haben Zugriff auf Daten –teilweise auch auf solche, die sie nicht bräuchten. Und auch wenn der IT-Schutzschild heutzutage hochgezüchtet und entsprechend resistent gegen Angriffe von aussen ist, so herrscht an einigen Orten innerhalb der Trutzburg noch einiges an Nachholbedarf, was die Informationsverwaltung und das Datenmanagement betrifft. Nur wenige Unternehmen kennen heutzutage eine griffige und klar definierte Klassifizierung von betrieblichen Dokumenten. Noch ein paar weniger kennen eine damit einhergehende Risikoabwägung, welche Dokumente nun für wen genau zugänglich sein sollen, und über welche, der Sensibilität der Information angemessenen, Kanäle diese auch verteilt werden dürfen. Auch bei den Prozessen, wie Mitarbeiter in heiklen Stellen in äusserst kritischen Positionen geschult und im Voraus überprüft werden, ist der Auszug aus dem Strafregister oftmals das höchste aller Gefühle.

Es wäre aber genau die Aufgabe eines umfassenden Informationssicherungskonzeptes, einen solchen integralen Ansatz zu fordern und fördern. Denn im Endeffekt ist das zu schützende Gut nicht primär der Computer des Angestellten, oder das Unternehmensnetzwerk, sondern die darauf fließende und abgelegte Information.

Wer bedroht denn nun was genau?

Auch wenn viele der oben erwähnten Beispiele eher plakativ und zugespitzt

dargelegt wurden, sollen sie vor allem ein Grundproblem etwas ausleuchten: Zum einen das Problem der Ubiquität von Daten und Informationen und die Tatsache, dass diese, auch wenn sie rein virtueller Natur sind, durch sehr wohl physische Aktionen manipuliert oder vereinnahmt werden können, oder aber relativ ungeschützt auf dem Silbertablett da liegen, falls es dem Angreifer gelingt, sich hinter dem IT-Schutzwall zu positionieren. Zum anderen sollen diese Beispiele aber auch darauf aufmerksam machen, dass es sehr wohl Daten gibt, die – richtig manipuliert – teils verheerende physische Effekte zeitigen können. Und genau hier liegt denn auch die eigentliche Antwort auf die im Titel gestellte Frage.

Es sind tatsächlich oft Akteure mit einer beträchtlichen kriminellen Energie, die sich der Informations- und Kommunikationsmittel bedienen, um an finanziell verwertbare Daten zu gelangen. Und es sind oft auch Staaten, die sich den Datendiebstahl zu Nutze machen, um etwas mehr über die Aktivitäten eines anderen Staates oder dessen Wirtschaft zu erfahren. Es sind aber auch Gruppierungen, welche nicht aus monetären sondern politischen Motiven gerne Zugriff hätten auf Computer, Prozesskontrollsysteme (so genannte SCADA-Systeme) und dergleichen. Und sei es nur, um im Vorfeld eines physischen Angriffes das Ziel besser kennenzulernen oder aber unter Umständen den Stecker übers virtuelle Schaltpult zur richtigen Zeit herauszuziehen.

Zwar gehört letzteres noch nicht zum *usus*, und das wird wohl auch noch ein bisschen auf sich warten lassen. Allerdings sind die vorhandenen Hinweise, dass sich auch politisch motivierte, extremistische Gruppierungen für Informations- und Kommunikationsmittel zu interessieren beginnen, nicht mehr von der Hand zu weisen. Und dies nicht nur, um Daten zu verschicken, sondern auch um Dinge unbrauchbar zu machen. So gilt denn im Endeffekt die alte Weisheit, dass angegriffen wird, was gewinnbringend

oder zumindest zielführend im Sinne der Angreifer ist. Und dabei entpuppt sich die zunehmende Verschmelzung von virtueller und realer Welt als wunderbares, neues Tummelfeld für Private, für Staaten und für andere Zeitgenossen, die per se nicht unbedingt Positives im Schilde führen. Und gerade die kritischen Informationsinfrastrukturen, die hier sehr breit gefasst sein sollen, sind ein lukratives Ziel für Spionage, Sabotage oder einfach die eigene Bereicherung. Und dabei wird in Zukunft vermehrt noch der Zugriff auf die Daten ins Zielfeld rücken, sei dieser nun über physische Mittel, via virtuelle Spielereien oder mit einer Kombination beider zu bewerkstelligen. Und so muss denn auch der Schutz der Information ins Zentrum gestellt werden, und dieser lässt sich je länger, je weniger nur mit Virenskannern, Firewalls und einem starken Passwort bewerkstelligen.

Marc Henauer



Marc Henauer ist Chef der Sektion MELANI/Cybercrime beim Dienst für Analyse und Prävention des Bundesamtes für Polizei (fedpol) im Eidgenössischen Justiz- und Polizeidepartement, Schweiz. Zuvor war er bei fedpol als Analytiker für Wirtschafts- und Internetkriminalität tätig. Er hat an der Universität St. Gallen Medien und Kommunikationsmanagement und an der Universität Zürich Wirtschaftswissenschaften studiert und den Master of Arts in Foreign Service an der Georgetown University, Washington DC, erlangt.

