02

Kapitel | Chapter

Forschungsausblick
Research Outlook

IAN T. BALDWIN
MAX-PLANCK-INSTITUT FÜR CHEMISCHE ÖKOLOGIE, JENA

Naturkunde im Zeitalter der Genomik: Wie man Molekularbiologen für Experimente im Freiland ausbildet

Fotos: D. Kessler, I.T. Baldwin und C. Diezel

1. AUF EINEN BLICK:

Pflanzen bilden die Grundlage von Nahrungsnetzen. Wir verstehen jedoch nur wenig von den genetischen Merkmalen, die ihnen das Überleben in der Natur ermöglichen - unser Wissen darüber stammt mehrheitlich aus Laborstudien mit einigen Modellorganismen. Jedoch unterscheiden sich die Lösungsansätze, die Pflanzen als Antwort auf die Herausforderungen ihrer Umgebung entwickelt haben, von Art zu Art. Darüber hinaus können Wechselwirkungen mit anderen Organismen, wie etwa Mikroben und Insekten, zusätzlich eine Rolle spielen.

Das Max-Planck-Institut für chemische Ökologie bildet *genome enabled field biologists* (in der Genomik geschulte Freiland-Biologen) aus, die versiert sind sowohl im Umgang mit modernen molekularbiologischen und experimentellen Methoden als auch mit der althergebrachten Disziplin der Naturbeobachtung. Sie nutzen Feldstationen und Freilandflächen gewissermaßen als Labore für das Studium von Genfunktionen.

Die Arbeiten haben gezeigt, dass Pflanzen eine Mehr-Stufen-Strategie verwenden, die sowohl den primären und sekundären Stoffwechsel als auch Nützlinge in Form von Prädatoren und Bestäubern involviert, um eines der Probleme zu lösen, das auch aus der Landwirtschaft bekannt ist: nämlich, wie man mit pflanzenfressenden Schädlingen fertig wird.

2. DER STAND DER FORSCHUNG AUF DIESEM GEBIET

Ein Ziel der biologischen Forschung im Zeitalter der Genomik ist, die Funktion von Genen genau zu verstehen. Die technologischen Fortschritte, die hier erzielt worden sind, sind eindrucksvoll. Moderne Molekularbiologie (Genomik, Transkriptomik, Proteomik, Metabolomik etc.), die auf Modellorganismen angewendet wird, liefert eine solche Fülle an Daten, dass - auf den ersten Blick - eine unvoreingenommene Analyse der Funktion biologischer Systeme möglich zu sein scheint. Allerdings reicht der technologische Fortschritt allein nicht aus, um eine Lebensform genau zu verstehen, und computergestützte Herangehensweisen wie die Systembiologie zur Deutung der „molekularen" Datenmengen sind von der Lösung dieser Aufgabe noch sehr weit entfernt.

Gene können auf allen hierarchischen Ebenen wirksam sein, in die sämtliche biologische Phänomene eingebettet sind: auf der Ebene der Zellen, der Gewebe, der Organe, der Organismen, der Populationen, der Arten, der Artgemeinschaften und schließlich der Ökosysteme. Ob ein Gen verloren geht, erhalten bleibt oder im Genom eines Organismus modifiziert wird, hängt davon ab, wie seine Expression die Darwin´sche Fitness des Organismus beeinflusst. Wir haben allerdings bei den meisten Genen bislang nur ihre biochemische Funktion definieren können, und diese kann mit der Funktion auf der Ebene des Organismus oder sogar darüber hinaus in Beziehung stehen – oder nicht.

Die den gesamten Organismus betreffende Funktion eines Gens aufzudecken, erfordert ein umfassendes und neues Verständnis des Organismus selbst. Die geringe Anzahl der bislang beforschten und sequenzierten Modellorganismen (in diesem Zusammenhang bezeichnet als „Expressionssysteme", z.B. Maus) und unser unvollkommenes Verständnis von deren naturgeschichtlicher Entwicklung haben die Analyse von Genfunktionen erheblich erschwert. Zum Beispiel ken-

* Verändert übernommen aus: Baldwin, I.T. (2012) Training a new generation of biologist: the genome-enabled field biologists. Proceedings of the American Philosophical Society, 156.2, im Druck.

nen wir die Naturgeschichte des biochemischen Expressionssystems Hefe nicht, sondern nur deren Physiologie im Erlenmeyerkolben und Brutschrank! Diese unglückliche Trennung der Biologie in Zell- und Molekularbiologie einerseits sowie Ökologie und Evolutionsbiologie andererseits, wie sie vor drei Jahrzehnten vollzogen wurde, hat zusätzlich zu dieser einseitigen Entwicklung beigetragen.

3. DIE CHANCEN DER FORSCHUNG

Der schnellstmögliche Fortschritt hin zu einer Analyse von Genfunktionen auf der Ebene des Organismus erfordert einerseits eine Anpassung computergestützter Forschung, andererseits aber eine Rückbesinnung auf die Vergangenheit der Biologie. In unserem Zeitalter der Genomik haben wir bedauerlicherweise die Fähigkeit verloren, Biologen mit einem „Gefühl für den gesamten Organismus" auszubilden. Die reine, genaue Naturbeobachtung, die einst im Vordergrund stand, verlor ihre Bedeutung, als der molekularbiologische Werkzeugkasten zur detaillierten Untersuchung einiger weniger Organismen, die dann auch noch durch Laborstudien domestiziert wurden, die „biologische Intuition" außer Acht ließ. Weil sich jedoch das Tempo neuer biologischer Entdeckungen in Modellorganismen inzwischen deutlich verlangsamt, besinnt sich die aktuelle biologische Forschung wieder auf die Beobachtung von Lebewesen in der freien Natur, tragischerweise genau zu dem Zeitpunkt, an dem unser Planet seinen sechsten und wahrscheinlich katastrophalsten Verlust an Artenvielfalt erlebt.

Die Zeit läuft uns davon. Wenn die Erde im Jahr 2050 neun Milliarden Menschen ernähren soll, wird der weitaus größte Teil der Produktivität unseres Planeten dazu benötigt werden, eine einzige Spezies, nämlich uns, mit Nahrung, Brennstoff, Wohnraum und Kleidung zu versorgen. Dabei wird für die übrigen erdbewohnenden Spezies nur wenig übrig bleiben, und wenn die meisten der natürlichen Lebensräume asphaltiert oder gepflügt sein werden, dann wird das biologische Erbe unseres Planeten für immer verloren sein.

Dieses Erbe ist das Ergebnis einer sich über sehr lange Zeiträume erstreckenden natürlichen Auslese. In den zahllosen, noch nicht kartierten Genomen von Lebewesen in der freien Natur liegt also die Lösung zu allen Problemen, mit denen sich Lebensformen in der Vergangenheit auseinandersetzen mussten. Das biologische Erbe ist unsere kollektive Bibliothek, die wir in einem noch nie dagewesenen Umfang verbrennen – im wörtlichen wie im metaphorischen Sinne. Fast alle dieser genetischen Bücher wurden noch nie geöffnet und in den verschwindend wenigen, die geöffnet worden sind, wurde nur Weniges gelesen und verstanden. Was diesen Verlust noch verschlimmert, ist die Tatsache, dass die genomische Revolution die Art und Weise, wie wir die genetische Information in dieser Bibliothek ausbeuten können, fundamental verändert hat: Es ist, als ob die einst fest gebundenen Lexika mit den genetischen Daten jeder einzelnen Art zu Sammlungen von Notizbüchern mit losen Blättern geworden sind, in denen nur einzelne Abschnitte (oder Gene) von einem Band in einen anderen verschoben und - dank der Fortschritte in der genetischen Manipulation - neu geordnet, zusammengefasst und kombiniert werden können.

Die naturkundliche Beobachtung und die Wertschätzung unseres biologischen Erbes gewinnen aber, wie schon gesagt, wieder an Bedeutung. Weil die Kosten für Gensequenzanalysen rapide sinken, ist die einst für undenkbar gehaltene Quantifizierung der Darwin´schen Fitness durch Zählen von vererbten Gensequenzen in den Genomen der Nachkommen finanzierbar geworden. Stellen Sie sich einfach die Darwin´sche Evolution als einen in die Zukunft fließenden Strom von DNA-Nukleotiden vor! Organismen bewegen diesen genetischen Strom weiter und die Darwin´sche Fitness misst die erfolgreiche Weitergabe von Genen. Organismen sind keine passiven Kabelkanäle, sondern die innovativen Versandunternehmen für den genetischen Strom, die immer wieder neue Wege finden, um ihre genetischen Lieferungen an die nächste Generation erfolgreicher zu gestalten – sei es pünktlicher, zuverlässiger oder effizienter. Die genetischen Merkmale, die die erfolgreichen „Lieferungen" in all die rauen und unwirtlichen Lebensräume des Planeten möglich machen, gehören zu den Schätzen des biologischen Erbes unseres Planeten, die darauf warten, entdeckt zu werden. Dieses Erbe ist die wertvolle Bibliothek, deren Bücher wir mit jeder neuen Golfanlage, jedem Häuserkomplex, jedem Skigebiet und jedem landwirtschaftlich genutzten Feld, mit denen wir die natürlichen Lebensräume immer weiter zurückdrängen, verbrennen.

DAS BIOLOGISCHE ERBE IST UNSERE KOLLEKTIVE BIBLIOTHEK, DIE WIR IN EINEM NOCH NIE DAGEWESENEN UMFANG VERBRENNEN – IM WÖRTLICHEN WIE IM METAPHORISCHEN SINNE. FAST ALLE DIESER GENETISCHEN BÜCHER WURDEN NOCH NIE GEÖFFNET UND IN DEN VERSCHWINDEND WENIGEN, DIE GEÖFFNET WORDEN SIND, WURDE NUR WENIGES GELESEN UND VERSTANDEN.

4. DIE AUSBILDUNG EINER NEUEN GENERATION VON BIOLOGEN

Angesichts der Möglichkeiten, die uns die Werkzeuge der genomischen Revolution an die Hand geben, und wegen des unmittelbar bevorstehenden Verlustes an Biodiversität müssen wir eine Generation genomisch geschulter Feldbiologen ausbilden, die mit dem molekularen Werkzeugkasten genauso vertraut ist wie mit der Kunst der genauen naturkundlichen Beobachtung. Mit anderen Worten: Wir müssen Biologen ausbilden, die sich, wie einst die berühmten Naturforscher des 19. Jahrhunderts, Alexander von Humboldt, Charles Darwin oder Ernst Stahl, dafür interessieren, wie Organismen mit den jeweiligen Herausforderungen ihrer Umgebung umgehen, heute aber ausgerüstet sind mit einem Biochip in der einen und einem Massenspektrometer in der anderen Tasche. Hierfür werden Graduiertenschulen erforderlich sein, die das Studium der Biologie wieder vereinheitlichen, indem sie die Darwin´sche Fitness als Kriterium zum Verständnis der Genfunktion verwenden und Feldstationen als „Labore" für genetisch definierte und manipulierte Organismen in ihren natürlichen Lebensräumen, d.h. genau dort, wo sich ihre genetischen Merkmale im Laufe der Evolution entwickelt haben, nutzen.

STELLEN SIE SICH EINFACH DIE DARWIN´SCHE EVOLUTION ALS EINEN IN DIE ZUKUNFT FLIESSENDEN STROM VON DNA-NUKLEOTIDEN VOR! ORGANISMEN BEWEGEN DIESEN GENETISCHEN STROM WEITER UND DIE DARWIN´SCHE FITNESS MISST DIE ERFOLGREICHE WEITERGABE VON GENEN.

Der Gegensatz zwischen dem unmittelbar drohenden Verlust an Artenvielfalt und der mangelnden Vertrautheit der meisten heutigen Biologen mit der Fähigkeit einer beobachtenden Naturforschung war für die Festlegung des übergreifenden Forschungsziels des Max-Planck-Instituts für chemische Ökologie in Jena bestimmend: Fortschritte in der Molekularbiologie in das Studium der ökologischen Interaktionen und umgekehrt das Wissen über den Gesamtorganismus in das Studium der Genfunktionen zu integrieren. Um dieses Ziel zu erreichen, bilden wir eine neue Generation von Biologen in einer wissenschaftlichen Umgebung aus, die den Zugang zu und die Unterstützung durch molekulare Methoden bietet, die wir speziell für die in Nordamerika heimische wilde Tabakpflanze *Nicotiana attenuata* entwickelt und aufgebaut haben. Diese Pflanzenart wurde wegen ihrer interessanten Ökologie und ihrer Fähigkeit, in einer ur-anfänglichen landwirtschaftlichen Nische zu gedeihen, ausgewählt. Indem untersucht wird, wie es dieser angestammten, „wilden" Pflanze gelingt, in einer Nische zu wachsen, in der wir heute auch unsere Nutzpflanzen anbauen (wenn auch mit sehr viel Pflege und umfangreichen Interventionen), erhalten wir Hinweise darauf, wie wir die „ökologische Intelligenz" unserer Kulturpflanzen erhöhen und sie autarker machen können.

Die langfristige und nachhaltige finanzielle Förderung durch die Max-Planck-Gesellschaft ermöglicht uns eine kontinuierliche Entwicklung von Methoden zur detaillierten Analyse von ökologisch wichtigen Eigenschaften der Pflanze unter realen Umweltbedingungen. Unsere Forschungsansätze werden durch die genetischen Eigenschaften vorgegeben, die den Pflanzen das Überleben in der Wildnis möglich machen. Die Verwendung von Pflanzen, die gentechnisch derart verändert sind, dass die Expression von wichtigen Genen für das Überleben im Ökosystem unterdrückt wurde, spielt eine zentrale Rolle bei unseren Experimenten. Die Freisetzungen erfolgen auf der Feldstation im Naturschutzgebiet Lytle-Ranch der amerikanischen Brigham-Young-Universität im Südwesten Utahs. Diese Feldstation in der Great Basin Wüste liegt im Zentrum des ursprünglichen Lebensraums des wilden Tabaks, das heißt: Sämtliche natürlichen Selektionsmechanismen, die das Genom dieser Pflanze geformt haben, sind vorhanden.

Unsere Ausbildung von genomisch geschulten Feldbiologen bietet ausreichend technische Unterstützung, damit Nachwuchswissenschaftler die genetische Grundlage eines ökologisch relevanten Merkmals ermitteln, seine Expression genetisch und phänotypisch manipulieren und nachfolgend untersuchen, welche Folgen diese Manipulation auf die Darwin´sche Fitness der Pflanze in ihrer natürlichen Umgebung hat – und dies alles im zeitlichen Rahmen einer in Deutschland einzureichenden Doktorarbeit. Den Wissenschaftlern muss die Vorstellung zusagen, in diesem relativ kurzen Zeitraum die Kluft zwischen dem genorientierten und dem feldbasierten Phänotyp zu überbrücken. Dies ist von großer Bedeutung, wenn nicht sogar die prägende Erfahrung in ihrer Ausbildung. Von solchen weitgefassten Forschungsthemen wird nämlich in den meisten biologisch ausgerichteten Graduiertenprogrammen eher abgeraten, weil der Fortschritt von Doktoranden gern in eng definierten, jedoch eben nur im „mechanistischen" Sinne gründlichen Dissertationen leichter zu bewerten ist.

Das Forschungsprogramm kombiniert die einzigartigen Vorzüge der Wissenschaftslandschaften in Deutschland und den USA: Die Max-Planck-Gesellschaft hat das gesamte Forschungsprogramm ermöglicht. Dies ist eine Leistung, die in den USA aus öffentlichen Mitteln kaum zu finanzieren gewesen wäre. Dagegen können in den USA Feldstationen und Naturreservate als offene „Labore" für das Studium der Genfunktion genutzt werden. Die Freisetzung gentechnisch veränderter Pflanzen ist zwar in den USA nicht weniger streng geregelt als in Europa. Allerdings ist mit der dort zuständigen Agentur (APHIS), die diese Feldversuche überwacht, ein sinnvoller wissenschaftlicher Dialog möglich, was im stark politisierten Genehmigungsumfeld in Deutschland inzwischen leider nicht mehr möglich ist. Die hervorragende Zusammenarbeit mit der Brigham-Young-Universität, dem Eigentümer und Betreiber des Lytle-Reservats, ist ein weiterer Schlüsselfaktor für den Erfolg des Programms. Der Forschungsertrag: mehr als 300 Veröffentlichungen in begutachteten wissenschaftlichen Zeitschriften.

Im nächsten Abschnitt fasse ich unsere Untersuchungsergebnisse über die Verteidigungsstrategien des wilden Tabaks zusammen, einer Pflanze, die sogar mit der Plage einer angepassten, resistenten Schadinsektenart fertig wird - und damit ein großes Problem der heutigen Landwirtschaft, nämlich die Resistenzbildungen von Schädlingen, längst gelöst hat.

5. DIE ABWEHR GEGEN ANGEPASSTE PFLANZENFRESSER WIRD AUF MEHREREN EBENEN ORGANISIERT

Alle ursprünglichen Wildpflanzen bilden wirksame Abwehrstoffe gegen eine Vielzahl von Pflanzenfressern, die versuchen, sich an ihnen gütlich zu tun. Der wilde Tabak produziert Nikotin, eine Substanz, die die Verbindung zwischen Nerven und Muskeln stört und gegen alle Angreifer wirksam ist - mit Ausnahme einer Handvoll Insekten, die sich auf Nikotin produzierende Pflanzen spezialisiert haben. Eines dieser Insekten ist die Larve des Tabakschwärmers *Manduca sexta*, einem Insekt, das die größte für Tiere je dokumentierte Nikotintoleranz hat: Die Raupe ist 700-mal resistenter als ein nikotinabhängiger Mensch.

Tabakpflanzen erkennen anhand bestimmter Komponenten im Speichel der Larven, dass sie von diesem Insekt angegriffen werden. Der Speichel gelangt in die Wunden der Blätter, während die Larven an ihnen fressen. Die Erkennung der Komponenten wird durch eine komplizierte Signalkette innerhalb der Pflanze verarbeitet, zu der bestimmte Rezeptoren, ein Kinase-Signalnetzwerk, eine Reihe von Transkriptionsfaktoren sowie ein Netzwerk von Phytohormonen gehören. Alle diese Elemente sind an einer auf fünf Ebenen abgestuften, höchst raffinierten Abwehrreaktion beteiligt.

DEN WISSENSCHAFTLERN MUSS DIE VORSTELLUNG ZUSAGEN, IN DIESEM RELATIV KURZEN ZEITRAUM DIE KLUFT ZWISCHEN DEM GENORIENTIERTEN UND DEM FELDBASIERTEN PHÄNOTYP ZU ÜBERBRÜCKEN. DIES IST VON GROSSER BEDEUTUNG, WENN NICHT SOGAR DIE PRÄGENDE ERFAHRUNG IN IHRER AUSBILDUNG.

Die erste Stufe dieser Abwehrreaktion besteht darin, die Herstellung von Nikotin zu drosseln. Nikotin kann von resistenten Pflanzenfressern nämlich als Nahrung oder sogar zu ihrer eigenen Verteidigung verwendet werden. Zur zweiten Stufe gehört die Bildung neuer Giftstoffe, gegen die die Larven empfindlich sind, zum Beispiel Substanzen aus der Familie der Phenolamine und der Diterpen-Glykoside (insgesamt etwa 30 neue Strukturen) sowie Verdauungshemmer vom Typ der Trypsin-(Proteinase-)Inhibitoren (TPIs). TPIs hemmen die Verdauungsenzyme der Larven und verlangsamen auf diese Weise das Larvenwachstum. Indem wir die Synthese bestimmter Verbindungen in Versuchspflanzen unterdrückten und Insekten, die zum Fressen auf diese Pflanzen gesetzt worden waren, anschließend untersuchten, konnten wir zahlreiche synergistische Effekte zwischen den verschiedenen pflanzlichen Abwehrstoffen entdecken.

In der dritten Stufe wird die Bildung einer Mischung flüchtiger organischer Verbindungen ausgelöst, bei der es sich im Wesentlichen um ein Duftgemisch handelt, das als „Alarmsignal" fungiert. Es liefert den Räubern, die sich von pflanzenfressenden Raupen ernähren, zuverlässige Informationen darüber, an welcher Stelle der Pflanze sich die Schädlinge befinden. Dies könnte man mit einem Hilferuf bei der Polizei vergleichen, wenn jemand in Gefahr ist. Die vierte Stufe geht der eigentlichen Ursache der Raupenplage auf den Grund, nämlich dass eine weibliche Motte ihre Eier auf die Pflanze gelegt hat, aus denen die Raupen hervorgegangen sind. Die Motte wurde durch den süßen Geruch der Blüten und die Aussicht auf Nektar angezogen, denn sie ist einer der Hauptbestäuber des wilden Tabaks. In der Natur kann es also kontrovers zugehen: Während die Larven schädlich sind, waren ihre El-

tern als Bestäuber nützlich. Um diese verhängnisvolle Liaison aufzulösen, bildet die Pflanze, nachdem sie die auslösenden Substanzen im Speichel der Larven wahrgenommen hat, einen neuen Blütentyp aus, der sich zu anderen Zeiten öffnet - diese Blüten öffnen sich während des Tages, im Gegensatz zu den nachts geöffneten Blüten, die die Motten anlocken, Und: die Tages-Blüten locken Kolibris als Bestäuber an! Kolibris legen keine Raupeneier und fressen keine Pflanzen. Durch den Wechsel ihres „Fortpflanzungssystems" verringert die Pflanze also die Zahl der von ihr angelockten pflanzenfressenden Insekten.

DIE NATUR IST DIE MUTTER DER ERFINDUNG, UND DIE ZEIT, DIE UNS NOCH BLEIBT, IHR WERK ZU ENTDECKEN UND ZU NUTZEN, DARF NICHT UNGENUTZT VERLOREN GEHEN.

Die fünfte Verteidigungsstufe ist eher eine Art von Toleranz- denn Verteidigungsreaktion. Sie wird aktiviert, wenn die vier ersten Verteidigungsebenen die Schädigung der Pflanze nicht einzudämmen vermochten. In dieser Stufe wird eine Veränderung des Nährstoffhaushalts in der Pflanze aktiviert, die bewirkt, dass der in der Photosynthese chemisch gebundene Kohlenstoff in den Wurzeln der Pflanze sicher gespeichert wird, statt zu den neu ausgebildeten Blättern – die von den hungrigen Larven sofort aufgefressen würden – in Form von Zuckern zu fließen. Wenn die Larven ausgewachsen sind und sich im Boden verpuppt haben, bedrohen sie die Pflanze nicht mehr - diese mobilisiert dann den in der Wurzel gespeicherten Kohlenstoff, um Blüten und Samen zu produzieren und die nächste Generation zu erzeugen.

Alle fünf Ebenen im Verteidigungssystem der Pflanze werden durch die Signalstoffe im Speichel der Larven aktiviert. Die Komplexität der Reaktionen und ihre Einbeziehung in sämtliche Aspekte des Stoffwechsels unterstreicht nicht nur, wie kreativ und innovativ der Vorgang der natürlichen Auslese bei der Suche nach Lösungen für umfassende Probleme sein kann (hier: Schädlinge, die nicht loszuwerden sind), sondern sie enthält auch Hinweise für Agrarwissenschaftler, wie man Nutzpflanzen züchten kann, die gegen Schädlinge dauerhaft resistent sind.

6. SCHLUSSBETRACHTUNG

Die künftigen Biologen werden den Verlust des größten Teils des biologischen Erbes unseres Planeten miterleben müssen, da immer mehr natürliche Lebensräume zerstört werden, um Platz für die explodierende Weltbevölkerung zu schaffen. Diese Lebensräume fungieren als Bibliotheken, in denen nicht nur Arten an sich aufbewahrt werden, sondern auch deren Lösungen für die komplexen Herausforderungen, die ihre Umwelt an sie stellt. Die Lebensräume können als „natürliche Labore" für das Studium von Genfunktionen dienen, oder mit anderen Worten: der wichtigsten noch ungelösten Fragen der Biologie. Die Max-Planck-Gesellschaft schult Biologen, die naturkundliches Know-how mit genomischen Methoden verbinden, sodass natürliche Lebensräume als Labore für eine Analyse der Genfunktion auf der Ebene des Gesamtorganismus genutzt werden können. Die Natur ist die Mutter der Erfindung, und die Zeit, die uns noch bleibt, ihr Werk zu entdecken und zu nutzen, darf nicht ungenutzt verloren gehen.

IAN T. BALDWIN
DEPARTMENT OF MOLECULAR ECOLOGY, MAX PLANCK INSTITUTE FOR CHEMICAL ECOLOGY, JENA, GERMANY

Natural history in the genomics era: training genome-enabled field biologists

1. AT A GLANCE:

Plants form the basis of all food webs, but we understand little about the traits that allow them to survive in nature. Our knowledge comes from laboratory studies with a few model plants; yet the solutions that plants have evolved to solve environmental challenges vary amongst taxa, and frequently involve associations with other organisms, such as microbes and insects.

The MPI for Chemical Ecology is training "genome enabled field biologists", adept at using the new "-omic" tools as well as the old-fashioned art of natural history discovery, to use field stations as laboratories for the study of gene function. This work has revealed that native plants use a multi-layered strategy that engages both primary and secondary metabolism as well as mutualistic predators and pollinators to solve a central problem of agriculture: how to cope with specialist herbivores.

2. STATUS OF THE FIELD

A central question for biology in this "genomics era" is to understand the function of genes and the technological advances toward this goal have been awesome. The "–omic" tools (genomic, transcriptomic, proteomic, metabolomic, etc.) that are being applied to model organisms are producing such volumes of data, that unbiased analyses of the function of complete biological systems seem possible. However, technology alone is not likely to be the only path forward. "Systems biology" and other computational approaches to making sense of all the "-omics" data are still a long way off.

Genes can function at all levels in the hierarchy in which all biological phenomena are embedded: cell, tissue, organ, organism, population, species, community, ecosystem. However, whether a gene is lost, maintained or modified in an organism's genome depends on how its expression influences the organism's Darwinian fitness. Despite the recognized central importance of the whole-organismic function of genes, for most genes, only their biochemical function is understood, and this biochemical function may or may not relate to their function(s) at the organismic level.

Uncovering the whole-organismic function of a gene requires an intimate understanding of the organism. The paucity of whole-organism expression systems and our incomplete understanding of the natural history of the organisms used in our biochemical expression systems have slowed the analysis of whole-organismic gene function. Failure to heal the unhappy divorce that split biology departments along cellular-molecular and ecological-evolutionary lines three decades ago has also contributed to the lackluster progress.

3. RESEARCH OPPORTUNITIES

The fastest way forward to an organismic level analysis of gene function will require adapting computational approaches, but also a return to the past. In this genomics era, we have lost our ability to train biologists with a "feel for the organism". The study of natural history lost its clout when the genetic (and later "–omic") tool box, used to pry open a handful of organisms domesticated for laboratory studies, invalidated "biological intuition". But as the pace of new biological discoveries from these model organisms slackens, natural history expertise is regaining its cache, tragically just as our planet is experiencing its 6th and likely, most devastating loss of biodiversity.

And we are rapidly running out of time. If the Earth is to support 9 billion people by 2050, the vast majority of the earth's primary productivity will be required to feed, fuel, house and clothe a single species, the resource-hungry *Homo sapiens*, and little will be left for the remaining inhabitants of the planet. And with most of the planet's natural habitats paved over or plowed under, our planet's biological legacy will be lost forever.

THIS BIOLOGICAL LEGACY IS OUR COLLECTIVE LIBRARY THAT WE ARE BURNING – LITERALLY AND FIGURATIVELY – AT AN UNPRECEDENTED RATE. ALMOST ALL OF THE BOOKS HAVE NEVER BEEN OPENED, AND THE VANISHINGLY FEW THAT HAVE, HAVE ONLY BEEN LIGHTLY BROWSED.

Our planet's biological legacy is the result of eons of natural selection. In the innumerable as-yet unmapped genomes of the natural world lie the solutions to the problems that life has faced in the past. This biological legacy is our collective library that we are burning – literally and figuratively -- at an unprecedented rate. Almost all of the books have never been opened,

* Adapted from: Baldwin, I.T. (2012) Training a new generation of biologist: the genome-enabled field biologists. Proceedings of the American Philosophical Society, 156.2, in press.

and the vanishingly few that have, have only been lightly browsed. To compound the loss, the genomics revolution has fundamentally altered how we can exploit the genetic information in this library; it's as if the once hard-bound lexicons of genetic information of each species have become collections of loose-leaf notebooks within which individual genes can be shuffled from one volume to another, reordered, recollated, recombined, thanks to advances in genetic manipulation.

Knowledge of natural history and the appreciation of our biological legacy is again on the rise. With sequencing costs plummeting, the once-elusive quantification of Darwinian fitness in a currency of sequence similarity becomes affordable. Think of Darwinian evolution as a stream of nucleotides flowing forward in time. Organisms move the genetic stream forward; their Darwinian fitness measures the success of this transmission. Organisms are not passive conduits but rather, the innovative Fed Ex employees of the genetic stream, finding new ways to make their genetic deliveries to the next generation more successful – more timely, more reliable, more economical. The traits that allow for these successful deliveries in all of the harsh and inhospitable habitats of the planet are just one of many treasures waiting to be discovered from our planet's biological legacy, this library that we are currently burning with every new golf course, housing complex and agricultural field that we build on natural habitats.

THINK OF DARWINIAN EVOLUTION AS A STREAM OF NUCLEOTIDES FLOWING FORWARD IN TIME. ORGANISMS MOVE THE GENETIC STREAM FORWARD; THEIR DARWINIAN FITNESS MEASURES THE SUCCESS OF THIS TRANSMISSION.

4. TRAINING A NEW GENERATION OF BIOLOGIST

Given both the opportunities provided by the tools of the genomics revolution and the urgency of our immediate loss of biodiversity, we need to train a generation of "genome-enabled field biologists (GEFBs)", who are adept at using the "-omic" tool box as well as intimate with the art of natural history discovery. In other words, we need to train biologists, who, like the famous biologists of 19th century, Alexander von Humboldt, Charles Darwin, and Ernst Stahl, are interested in how organisms solve environmental challenges, but now have a microarray in one pocket and a mass spectrometer in the other. This will require graduate training programs that reunify the study of biology by using Darwinian fitness as the criteria for understanding gene function, and field stations that can be used as "laboratories" with genetically defined and manipulated organisms in the habitats in which they evolved.

The stark juxtaposition of the immediacy of our biodiversity loss and the lack of familiarity of most modern biologists with the skills required for natural history discovery has motivated the overarching scientific objective of the Max Planck Institute for Chemical Ecology in Jena, Germany: to integrate advances in molecular biology into the study of ecological interactions and in turn, to integrate ecologists' whole-organismic expertise into the study of gene function. To accomplish this, we are training a generation of GEFBs in a scientific environment that offers access to and support in the use of molecular tools that have been developed for a native tobacco plant (*Nicotiana attenuata*), chosen for its interesting ecology, and ability to thrive in the primordial agricultural niche. By studying how this native plant manages to thrive in the niche in which we grow our agricultural plants (albeit with much pampering and many inputs), we hope to learn how to increase the "ecological intelligence" of our crop plants to make them more self-sufficient.

The long-term, patient funding of the Max Planck Society has allowed us to develop tools that enable ecologically important traits to be genetically dissected and manipulated under "real-world" conditions. Our research interests are broadly defined by the traits that allow plants to survive in nature. Releases of plants genetically modified to silence the expression of genes important for ecological performance at our field station at Brigham Young University's Lytle Ranch Preserve in southwestern Utah (USA) play a central role in the research. This field station in the Great Basin Desert lies in the center of *N. attenuata's* native habitat and includes all of the natural selective pressures that have sculpted this plant's genome.

Our approach to the training of GEFBs is to provide sufficient technical support so that students have the potential of identifying the genetic basis of an ecologically relevant trait, manipulate its expression genetically and phenotypically and examine the consequences of these manipulations for the plant's Darwinian fitness in its natural environment, all within the timeframe of a German Ph.D. thesis. To feel comfortable spanning the chasm between gene and field-based phenotype in a short period of time is a centrally

important, if not formative experience in the training of a GEFB. Such broadly formulated thesis questions are usually discouraged in most biology graduate programs, as a student's progress in a narrowly defined but mechanistically deep thesis is easier to evaluate.

This research program combines strengths unique to the German and US scientific environments. The long-term patient funding of the Max Planck Society has enabled the entire research program, but particularly the development of the molecular toolbox for this native plant, a feat nearly impossible to finance from public sources in the US. Only in the US, where the release of genetically modified plants is regulated no less rigorously than it is in Europe, but by an agency (APHIS) with which a scientifically coherent dialogue is possible, can field stations and nature preserves be used as laboratories for the study of gene function; this is not possible in the highly politicized regulatory environment in Germany. An excellent working relationship with Brigham Young University, which owns and operates the Lytle Preserve, has also been a key determinant of the success of the program. The research has produced more than 300 peer-reviewed publications and next I summarize what our research has revealed about how a native plant copes with plagues of adapted insect pests: the central challenge for agriculture.

5. RESISTANCE AGAINST ADAPTED HERBIVORES IS ORGANIZED IN MULTIPLE LAYERS

All native plants produce effective defenses against the multitudes of generalist herbivores that try to make a living eating their tissues. *N. attenuata* evolved the ability to synthesize nicotine, a toxin that poisons the neuromuscular junction and is an effective poison against all mobile attackers, except the handful of insects that have specialized on nicotine-producing plants. One of these insects is the larvae of *Manduca sexta*, an insect that holds the record for nicotine tolerance (being 700 times more resistant than a nicotine-addicted human).

N. attenuata can tell when it is attacked by this insect by detecting particular compounds in the spit of the larvae, compounds that are introduced into wounds as the larvae chews on leaves. These compounds are recognized by a complicated signal transduction pathway that involves specific receptors, a kinase signaling network, a suite of transcription factors and a network of phytohormones, all of which are responsible for eliciting a five-layered, graded and highly sophisticated defense response.

The first stage in this defense response is to shut down the production of nicotine; nicotine can be metabolized by this nicotine-resistant herbivore to provide nutrients or sequestered for its own defense. The second stage involves the production of a new suite of toxins to which the larvae are sensitive, such as the family of phenolamines and diterpene glycosides, about 30 new structures, as well as a group of digestibility reducers, such as the trypsin proteinase inhibitors (TPIs). TPIs inhibit the larvae's ability to digest leaf proteins and slow larval growth. By silencing the production of one group of compounds and querying the herbivores, we have uncovered many defensive synergies amongst these different defense metabolites.

TO FEEL COMFORTABLE SPANNING THE CHASM BETWEEN GENE AND FIELD-BASED PHENOTYPE IN A SHORT PERIOD OF TIME IS A CENTRALLY IMPORTANT, IF NOT FORMATIVE EXPERIENCE IN THE TRAINING OF A GENOME ENABLED FIELD BIOLOGIST.

The third stage is to elicit the production of a complex bouquet of volatile organic compounds, essentially a perfume that functions as an "alarm call" that provides reliable information to the predators of the larvae about their location on the plant. This is akin to "calling the police". The fourth stage addresses how the larvae arrived on the plant in the first place: when an adult female moth laid an egg on the plant. Adult moths are actively attracted by the sweet-smelling scent released by the flower and the promise of a nectar reward; the moth is one of the plant's main pollinators. Most things in nature are complicated; harmful lavae frequently have beneficial parents. To uncouple this association, the plant, after sensing the elicitors in larval spit, produces a new type of flower with a different flower opening time. This flower opens during the day (in contrast to the night-opening flower that attracts the moth) and this flower attracts hummingbirds as pollinators. Hummingbirds do not lay insect eggs and are not herbivores. Hence by switching its sexual system, the plant reduces the number of herbivores it recruits.

The fifth stage of defense is more a type of tolerance response than a defense response and is activated when the first 4 defensive layers are not effective in reducing a plant's damage. In this stage, the elicitors activate a change in the

plant's source-sink relationships, so that recently fixed carbon from photosynthesis, rather than being transported to newly developed leaves (which are readily eaten by hungry larvae), are bunkered in the roots where it's safely stored. Once the larvae have grown and pupated in the soil, they are no longer a threat to the plant and the plant remobilizes this root stored carbon to produce new flowers and seeds.

All 5 of these layers in the plant's defense department are activated by the elicitors in the spit of the larvae. The complexity of the responses and their engagement of all aspects of metabolism and physiology underscores not only how creative and innovative the process of natural selection can be in finding solutions to complex problems (pests that will not go away) but suggests many avenues that agronomists might take to engineer crop plants with durable resistance against agricultural pests.

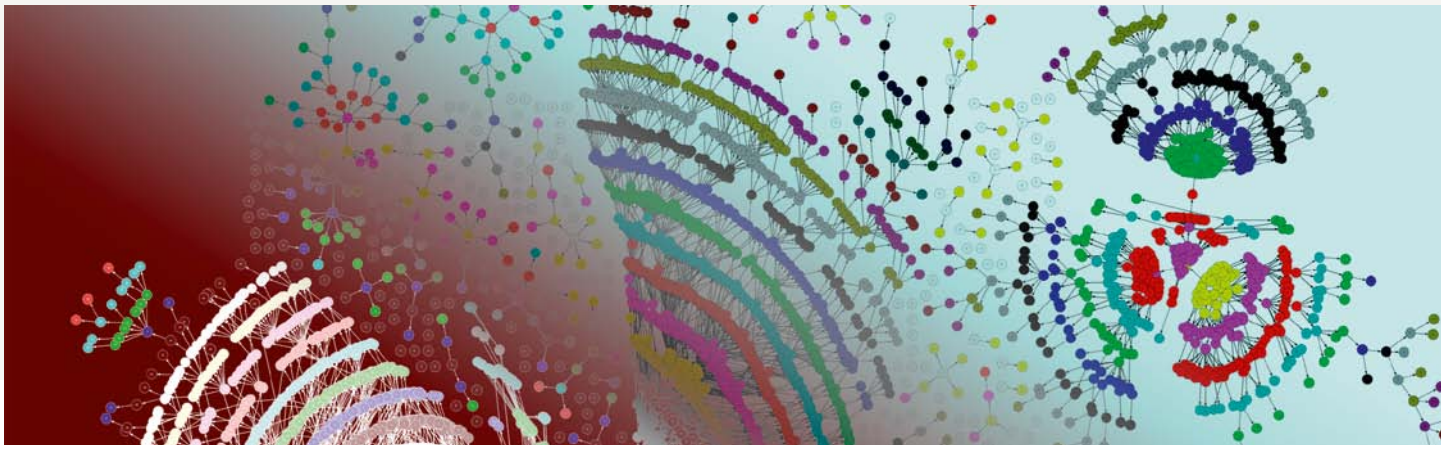
NATURE IS THE MOTHER OF INVENTION AND WE ARE RUNNING OUT OF TIME TO DISCOVER AND USE HER HANDIWORK.

6. CONCLUSION

The current generation of biologists will oversee the loss of the majority of our planet's biological legacy as natural habitats are destroyed to make room for the exploding human population. These habitats function as libraries, preserving species and the solutions these species have evolved to complex environmental problems. These habitats can also serve as natural laboratories for the study of gene function: the major unsolved question in biology. The Max Planck Society is training biologists to combine natural history know-how with genomic tools to use natural habitats as laboratories for an organismic-level analysis of gene function. Nature is the mother of invention and we are running out of time to discover and use her handiwork.

KRISHNA GUMMADI, PETER DRUSCHEL, PAUL FRANCIS
MAX-PLANCK-INSTITUT FÜR SOFTWARESYSTEME, KAISERSLAUTERN UND SAARBRÜCKEN

Social Computing



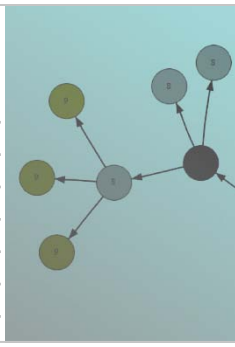
1. EINLEITUNG

Im Arabischen Frühling haben Twitter und Facebook in der Verbreitung von Informationen und der Organisation von Protesten eine signifikante Rolle gespielt. Justin Bieber wurde zum umschwärmten Teeniestar, nachdem er Videos von sich auf YouTube eingestellt hatte. Jeder kann auf Seiten wie Amazon und Netflix Rezensionen einstellen, um so fremde Leute bei ihrer Kaufentscheidung zu beraten. In den USA werden die sozialen Medien dazu verwendet, um sogenannte „Flash Robs" zu organisieren. Dabei werden Menschen aufgerufen, sich beispielsweise bei einem bestimmten Laden zu treffen und dort dann Waren zu stehlen. Diese Beispiele zeigen deutlich, dass die Informationstechnologien und die sozialen Medien mittlerweile einen erheblichen Einfluss auf die Gesellschaft ausüben.

Beim Social Computing handelt es sich um ein neu entstehendes Forschungsgebiet, das diese und andere Phänomene erforscht, die entstehen, wenn Menschen unterstützt durch die Informationstechnologie miteinander interagieren, zusammenarbeiten und konkurrieren. Diese Formen der durch Informationstechnologie vermittelten sozialen Interaktion spielen eine zentrale Rolle im heutigen Internet, das sich zu einer globalen Multimedia-Plattform für Kommunikation, soziale Netzwerke, Unterhaltung, Ausbildung, Informationen, den Handel, politischen Aktivismus und Selbstdarstellung entwickelt hat.

In den vergangenen zehn Jahren hat die sogenannte „Ära des Social Computing" begonnen. Im Vergleich zum frühen Internet sind die heutigen Internetnutzer keine passiven Konsumenten von Informationen und Dienstleitungen mehr, die von professionellen Informationsquellen und Serviceprovidern angeboten werden. Die heutigen Nutzer veröffentlichen selbst Multimediainhalte auf Seiten wie YouTube, partizipieren in sozialen Netzwerken wie Facebook oder handeln mit Waren und Dienstleistungen in Auktionshäusern wie eBay. Sie teilen auf Shopping- und Buchungsseiten Meinungen und Erfahrungen in Bezug auf Produkte, bringen ihr Wissen und ihre Kompetenz in Blogs und auf Wikipedia ein, verbreiten ihre Gedanken über Twitter und bieten ihre freiberuflichen Dienstleistungen über Auftragsauktionsseiten wie beispielsweise Mechanical Turk an. Faktisch nutzt das moderne Internet die Informationstechnologie, um eine virtuelle Plattform bereitzustellen, die von den Menschen in der kompletten Bandbreite sozialer Aktivitäten genutzt wird. Die Ära des Social Computing bringt jedoch auch neue Gefahren mit sich. Die beispiellose Menge an gesammelten Informationen über Aktivitäten und Vorlieben des Einzelnen kann auch für negative Zwecke verwendet werden. Personalisierte Informationsdienstleistungen, die auf die bekannten Interessen des Einzelnen ausgerichtet sind, können zu sogenannten „filter bubbles" führen, in denen die Nutzer nur wenige Informationen erhalten, die ihren Blickwinkel erweitern oder ihre Sicht der Dinge verändern könnten. Und:

PERSONALISIERTE INFORMATIONSDIENSTLEISTUNGEN, DIE AUF DIE BEKANNTEN INTERESSEN DES EINZELNEN AUSGERICHTET SIND, KÖNNEN ZU SOGENANNTEN „FILTER BUBBLES" FÜHREN, IN DENEN DIE NUTZER NUR WENIGE INFORMATIONEN ERHALTEN, DIE IHREN BLICKWINKEL ERWEITERN ODER IHRE SICHT DER DINGE VERÄNDERN KÖNNTEN.

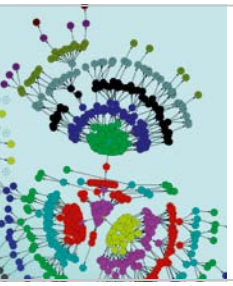


die Menschen vertrauen verstärkt auf den online geführten sozialen Diskurs – vermutlich auf Kosten der sozialen Interaktionen in der realen Welt.

Die Beliebtheit sozialer Onlineangebote, die von der ansteigenden Nutzung von Smartphones, anderen mobilen Geräten und einem allgegenwärtigen Internetzugang in großen Teilen der Welt noch verstärkt wird, hat einen profunden Einfluss auf die Weltwirtschaft und das Gefüge der Gesellschaft:

Soziale Beziehungen: Die Informationstechnologie ermöglicht und unterstützt Online-Communitys, die über das Potenzial verfügen, die Lebensqualität der Menschen zu verbessern, die Produktivität der Gesellschaft zu erhöhen sowie den Informationsaustausch und den politischen Diskurs zu demokratisieren. Die Forschung im Bereich des Social Computing untersucht die Organisation und die Entwicklung von Online-Communitys sowie die Prinzipien, die der Gestaltung sozialer Dienste zur effektiven Nutzung von Online-Communitys zugrunde liegen.

Informationsverbreitung: Die Online-User vertrauen verstärkt den Aussagen anderer Online-User, anstatt in Bezug auf Informationen und Orientierungshilfen auf traditionelle Instanzen wie die Medien, Unternehmen, den Staat, politische Parteien und religiöse Organisationen zu vertrauen. Die Forschung im Bereich des Social Computing will die Prinzipien und die Mechanismen erforschen, nach denen in der Online-Welt ein Informationsfluss stattfindet, sich Meinungen verbreiten und die Menschen beeinflusst werden.



SOCIAL COMPUTING IST EIN NEU ENTSTEHENDER FORSCHUNGSZWEIG, DER DIE PHÄNOMENE UNTERSUCHT, DIE ENTSTEHEN, WENN MENSCHEN ÜBER INFORMATIONSTECHNOLOGIE INTERAGIEREN, ZUSAMMENARBEITEN ODER KONKURRIEREN.

Neue Gefahren: Die sozialen Informationstechnologien führen zu möglichen Problemen hinsichtlich der Privatsphäre, der Sicherheit und der Freiheit der Menschen. Sie schaffen neue Wege der Manipulation und Fehlinformation und bergen die Gefahr von Filter Bubbles, sozialer Isolation in der realen Welt und einer Verschärfung des „digital divide", der Kluft zwischen Menschen mit und ohne Internetzugang mit sich. Die Forschung im Bereich des Social Computing sucht diese Gefahren zu erforschen sowie soziale, technologische, rechtliche und wirtschaftliche Gegenmaßnahmen zu entwickeln.

Social Computing erforscht im weitesten Sinn die Möglichkeiten und Herausforderungen, die entstehen, wenn soziale Aktivitäten der Menschen durch die Informationstechnologie unterstützt und transformiert werden. Dieses neu entstehende interdisziplinäre Forschungsgebiet überschneidet sich mit der Informatik, den Sozialwissenschaften, den Rechtswissenschaften und den Wirtschaftswissenschaften. Einige der untersuchten Schlüsselphänomene umfassen das soziale Netzwerken, den Austausch von Inhalten und das Bloggen, die Social Peer Production und das Crowd-Sourcing, Onlinespiele und virtuelle Welten in Bezug auf Unterhaltung und Ausbildung, den Online-Handel, Auktionen und Werbung, den Online-Datenschutz und die Nutzerverantwortlichkeit, sowie Spam und die Internetkriminalität.

Bei Network Science handelt es sich um ein verwandtes interdisziplinäres Forschungsgebiet (das Informatiker, Physiker, Mathematiker und Wissenschaftler anderer Disziplinen einschließt), das sich auf die Erforschung physikalischer, biologischer, technischer und sozialer Phänomene konzentriert, die als komplexe Graphen oder Netzwerke dargestellt werden können. Der Bereich überschneidet sich mit dem Social Computing in seiner Forschung im Bereich sozialer Netzwerke. Network Science konzentriert sich hier auf die Grapheigenschaften sozialer Netzwerke, wohingegen das Social Computing die gesamte Bandbreite der technischen, wirtschaftlichen und sozialen Aspekte dieser und anderer Systeme betrachtet.

Wir geben in diesem Artikel einen Überblick über die Schlüsselherausforderungen und -möglichkeiten in dem neu entstehenden Forschungsgebiet des Social Computing aus der Perspektive der Menschen, der Wirtschaft und der Gesellschaft, sowie einen Ausblick auf die Zukunft dieses spannenden interdisziplinären Forschungsgebiets. Es ist jedoch wichtig, darauf hinzuweisen, dass Social Computing einerseits viele Forschungsbereiche umspannt, andererseits aber noch in den Kinderschuhen steckt. Wissenschaftler verschiedener beteiligter Forschungsgebiete vertreten daher noch unterschiedliche Meinungen zu den Kernfragen und Herausforderungen und dazu wie sich das Forschungsgebiet entwickeln wird. Dieser Artikel reflektiert vornehmlich die Sichtweise der Autoren als Informatiker.

2. HINTERGRUND

Wir beginnen mit einer kurzen Beschreibung einiger der beliebtesten sozialen Systeme und Angebote des heutigen Internets, um somit einen Hintergrund für unsere Diskussion über die Schlüsselherausforderungen und -möglichkeiten des Social Computing zu geben.

2.1 SOZIALE ONLINE-NETZWERKE UND DER AUSTAUSCH VON INHALTEN

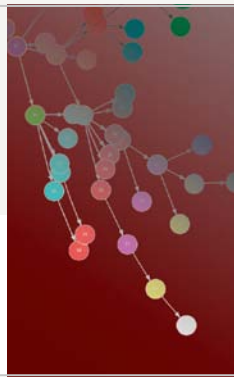
Soziale Online-Netzwerke (OSN) wie Facebook und ihre vielen spezialisierteren oder regionalen Mitbewerber zählen heute zu den beliebtesten Online-Services. Allein Facebook beansprucht für sich, über 845 Millionen Nutzer zu verfügen (Stand Dezember 2011). Die OSNs ermöglichen es dem Nutzer, anzugeben, wer zu seinen Freunden gehört oder wer seine Arbeitskollegen sind, und das resultierende soziale Netzwerk zu betrachten. Es ermöglicht den Nutzern, Informationen über sich und ihre Aktivitäten mit Freunden, Freunden von Freunden und der Öffentlichkeit austauschen zu können. Die OSNs verschärfen den Konflikt zwischen dem Wunsch der Menschen, sich einerseits mitzuteilen und andererseits die Privatsphäre zu bewahren. Dies veranlasst die Nutzer oftmals dazu, sensible Daten in einer nicht beabsichtigten oder abträglichen Art und Weise preiszugeben.

Internet-Videoportale wie YouTube ermöglichen es den Usern, ihre Videos mit Freunden und der Öffentlichkeit austauschen zu können. Diese Videos können von den Usern selbst (z.B. eigene kreative Arbeiten, Bildmaterial von Ereignissen oder „How-to"-Anleitungen) oder von anderen produziert worden sein. Die Nutzer können Videos empfehlen und die Empfehlungen anderer dazu verwenden, Videos, die ihnen gefallen könnten, zu finden. Dadurch können sich bestimmte Videos „viral" verbreiten, was einem normalen Nutzer erlaubt, Videos zu produzieren und ins Netz zu stellen, die dann von Millionen Menschen gesehen werden, und so womöglich zu einem Online-Star zu avancieren.

2.2 BLOGS UND MIKROBLOGS

Blogs sind eine Art persönliches Tagebuch, die es den Verfassern ermöglichen, Informationen und Gedanken über ihr Leben oder über ein spezifisches Thema der interessierten Öffentlichkeit oder bestimmten Online-Freunden mitzuteilen. Blogs von Prominenten, Politikern oder Experten sind ungemein beliebt. Diesen Blogs folgen in vielen Fällen Millionen Menschen. Twitter bietet die Möglichkeit des Mikrobloggings an. Die Nutzer können hier kurze Textnachrichten, sogenannte Tweets, von ihren Handys aus veröffentlichen. Diese werden dann in Echtzeit an die Follower, also an Menschen, die angegeben haben, die Tweets des Users erhalten zu wollen, weitergeleitet. Twitter verfügt über 100 Millionen aktive Nutzer und leitet über 230 Millionen Tweets pro Tag weiter (Stand September 2011).

FACEBOOK HAT 845 MILLIONEN NUTZER, TWITTER VERFÜGT ÜBER 100 MILLIONEN AKTIVE NUTZER UND LEITET ÜBER 230 MILLIONEN TWEETS PRO TAG WEITER. DER ONLINEHANDEL ERZIELT 8 % DER VERKÄUFE DES US-AMERIKANISCHEN EINZELHANDELS IN 2011. DARÜBER HINAUS GEHT MAN DAVON AUS, DASS SICH DIE ONLINE-VERKÄUFE BIS ZUM JAHR 2015 VERDOPPELN WERDEN.



2.3 ONLINEHANDEL: SHOPPING UND AUKTIONEN

Onlineshops wie Amazon bieten eine Vielzahl von Produkten zum Kauf an. Die Kunden haben zusätzlich zu den üblichen Produktbeschreibungen Zugang zu Empfehlungen und Rezensionen anderer Kunden, die ein Produkt bereits erworben haben. Darüber hinaus verfolgt Amazon das Surf- und Einkaufsverhalten der Kunden, um so neue Produkte, die den Kunden vielleicht interessieren könnten, vorzuschlagen. Online-Auktionshäuser wie eBay ermöglichen es den Kunden, ihre eigenen Waren anbieten und auf die Angebote anderer Kunden bieten zu können. Das System speichert Bewertungen der Kunden sowohl über die Verkäufer als auch über die Käufer, um die Kunden vor potenziellen Betrügern warnen zu können. Onlineshops sind ungemein populär geworden. Der Onlinehandel erzielt einen geschätzten Jahresumsatz in Höhe von 142,5 Milliarden US Dollar. Dies macht 8 % der Verkäufe des US-amerikanischen Einzelhandels in 2011 aus. Darüber hinaus geht man davon aus, dass sich die Online-Verkäufe bis zum Jahr 2015 verdoppeln werden.

2.4 PEER-PRODUCTION- UND CROWD-SOURCED-SYSTEME

Bei Wikipedia handelt es sich um ein Beispiel für ein Peer-Production-System. Wikipedia ist eine Online-Enzyklopädie, bei der Einträge ausschließlich von Freiwilligen geschrieben, editiert und gepflegt werden. Die meisten Einträge können von jedem Nutzer verändert werden. Die verantwortlichen freiwilligen Redakteure überprüfen dann Änderungen und neue Einträge. Die Redakteure sind oftmals lediglich unter einem Online-Pseudonym bekannt. Die Nut-

zergemeinschaft vertraut ihnen aufgrund ihrer Leistungen in der Vergangenheit anstatt jedweder formeller Referenzen. Die Nutzer werden um Spenden gebeten, um die Kosten für den Betrieb der technischen Infrastruktur zu decken.

MAN KANN ÜBER DIE BEDEUTUNG VON SOZIALEN NORMEN IN DER ONLINE-WELT UND IM REALEN LEBEN STREITEN, ABER NUTZER SIND MÖGLICHERWEISE EHER GENEIGT, IHRE MEINUNGEN UND IHRE PERSÖNLICHEN INFORMATIONEN IN DER ONLINE-WELT ALS IN DER REALEN WELT KUNDZUTUN.

Ein weiteres Beispiel für ein Peer-Production-System ist Mechanical Turk. Hierbei handelt es sich um Auftragsauktionen. Der Service bietet Unternehmen, Entwicklern und Wissenschaftlern eine nach Bedarf verfügbare und beliebig ausbaubare Arbeiterschaft, indem sie Nutzer vermittelt, die sogenannte human intelligence tasks (HITs) gegen ein Entgelt übernehmen wollen. Eine typische Aufgabe ist, Fotos mit Schlüsselwörtern zu versehen, die am besten deren Inhalt beschreiben. Diese Aufgabe ist für Menschen leicht, für heutige Computer aber sehr schwer lösbar. Mechanical Turk kombiniert die Stärke der Informationstechnologie (die Handhabung großer Mengen an Daten und die Fähigkeit, Aufgaben mit Dienstleistern zusammenzuführen, wo immer diese weltweit verfügbar sind) mit den Fähigkeiten und Möglichkeiten der Menschen.

2.5 ONLINE-WERBUNG

Die Nutzer können einen großen Teil der Dienstleistungen im Internet kostenlos nutzen. Unternehmen (einschließlich Facebook, Google, Yahoo etc.), die diese Dienstleistungen anbieten, erzielen ihren Umsatz aus dem Verkauf von Anzeigen. Online-Anzeigen erzielen hohe Preise in der Werbebranche. Dies liegt daran, dass die Nutzer viel Zeit im Internet verbringen und zum Teil auch daran, dass die Anzeigen anhand der gegenwärtigen Aktivitäten (z. B. Suchanfragen) oder dem Profil eines Nutzers gezielt platziert werden können. Suchmaschinen wie Google und Bing erstellen solche Nutzerprofile anhand von Suchanfragen und Website-Besuchen, Web-E-Mail-Anbieter wie Gmail oder HotMail nutzen die Inhalte der Nutzer-E-Mails und OSNs wie Facebook nutzen die Angaben ihrer Nutzer zur Person.

3 SCHLÜSSELHERAUSFORDERUNGEN DER FORSCHUNG

In diesem Abschnitt diskutieren wir die wesentlichen Fragen und Schlüsselherausforderungen der Social Computing-Forschung, die sich durch die im vorherigen Abschnitt diskutierten sozialen Systeme und Dienstleistungen stellen.

3.1 SOZIALE BEZIEHUNGEN UND DARSTELLUNG IM INTERNET

Die Social Computing-Technologien haben es den Menschen erleichtert, über physikalische Entfernungen hinweg mit ihren sozialen Gruppen zu kommunizieren, Kontakt aufzunehmen und Informationen auszutauschen. Die Nutzer können mittels sozialer Netzwerke wie Facebook in Kontakt mit ihren Familien und Freunden bleiben und etwa alte Freunde oder Arbeitskollegen wiederfinden. Diese Services fördern Online-Interaktionen durch den Austausch von Status-Updates und Inhalten, welche die sozialen Gefüge verstärken und die Menschen dabei unterstützen, Beziehungen über Entfernungen hinweg eingehen, aufbauen und pflegen zu können.

Die intensive Nutzung sozialer Online-Services, besonders durch die jüngeren Generationen, kann andererseits zulasten ihrer sozialen Interaktionen in der realen Welt gehen. Es hat in der Tat den Anschein, als verändere die Popularität der sozialen Online-Interaktionen die vorherrschenden sozialen Normen dahin gehend, wie Menschen mit anderen Menschen interagieren und welche Informationen sie mit wem austauschen. Man kann über die Bedeutung von sozialen Normen in der Online-Welt und im realen Leben streiten, aber Nutzer sind möglicherweise eher geneigt, ihre Meinungen und ihre persönlichen Informationen in der Online-Welt als in der realen Welt kundzutun. So handelt es sich bei vielen Inhalten, die auf sozialen Seiten ausgetauscht werden, um persönliche Multimedia-Inhalte wie Fotos und Videos von Familienurlauben oder Betriebsfeiern. Darüber hinaus sind die Inhalte oftmals vielen zugänglich. Dies gefährdet die Privatsphäre der Nutzer und verstärkt die Wirkung sozialen Fehlverhaltens wie beispielsweise Mobbing, Verleumdungen oder Stalking.

Eine Schlüsselherausforderung für die Forschung ist es, zu verstehen, wie soziale Online-Services das soziale Gefüge von Online- und Offline-Beziehungen beeinflussen und wie der Austausch persönlicher Online-Informationen die sozialen Normen in Bezug auf den Datenschutz sowohl verletzen als auch ändern können.

3.2 DIE DEMOKRATISIERUNG DES PUBLIKATIONSPROZESSES UND DIE MUND-ZU-MUND-PROPAGANDA

Die geringen Speicher- und Übertragungskosten für digitale Daten haben Sites wie YouTube, auf denen man Inhalte austauschen kann, ermöglicht. Diese haben im Weiteren die Publikation von Inhalten demokratisiert. Bei YouTube sind Beiträge von Millionen Nutzern weltweit eingestellt, zu einer Vielzahl an Themen von kreativen Performances über persönliche Nachrichten-Accounts bis hin zu Diskussionen über spezifische Themen wie die Quantenphysik. Die Nutzer produzieren Videos, in denen sie sich äußern, wobei die Bandbreite vom Banalen (Diskussionen über Fernsehsendungen) über Schulungen (Gitarrenstunden) bis hin zur Politik (Aufruf zur Auflehnung gegen etablierte Obrigkeiten) reicht.

Darüber hinaus können Inhalte, welche von normalen Usern veröffentlicht wurden, von anderen Usern durch „Mund-zu-Mund-Propaganda" verbreitet werden. Die Nutzer tauschen jeden Tag Hunderte Millionen URLs (Links zu Websites, Blogs, YouTube Videos), die sie entdecken, mit ihren Freunden und Followern über Facebook und Twitter aus. Die sozialen Computing-Technologien demokratisieren daher die Veröffentlichung von Inhalten sowie deren Verbreitung, indem sie es jedem Nutzer ermöglichen, eigene Inhalte in sozialen Online-Netzwerken zu veröffentlichen und diese durch andere Nutzer mittels Mund-zu-Mund-Propaganda verbreiten zu lassen.

Hier ist es eine Schlüsselherausforderung für die Forschung, die Dynamik der Mund-zu-Mund-Propaganda zu verstehen und zu erforschen, wie man Gerüchte und Lügen von wahren Geschichten differenziert und wie die Nutzer die Glaubwürdigkeit einer Quelle feststellen. Dieses Verständnis ist elementar wichtig für unser Vermögen, soziale Systeme zu entwerfen, die relevante und zuverlässige Informationen bereitstellen.

3.3 NUTZUNG DER „WISDOM-OF-CROWDS", UM RELEVANTE INFORMATIONEN ZU FINDEN

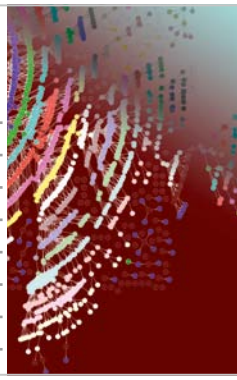
Soziale Services können neben der Veröffentlichung von Inhalten die Wisdom-of-Crowds (also das Feedback vieler Menschen) nutzen, um relevante Informationen zu finden. So werden beispielsweise die User-Bewertungen der YouTube-Videos im Wesentlichen dazu verwendet, die Suchergebnisse für YouTube-Videos zu priorisieren. Amazon verfährt ähnlich. Der Onlineshop von Amazon empfiehlt Nutzern Bücher anhand der Bücher, die der Nutzer bereits zu einem früheren Zeitpunkt gekauft hat, sowie anhand der Produkte, die andere Nutzer, die dieses Buch gekauft haben, auch noch gekauft haben.

Empfehlungen von Menschen mit den gleichen Interessen unterscheiden sich in mehrfacher Hinsicht von traditionellen Empfehlungen einer kleinen Anzahl bekannter Experten (etwa Redakteure von Tageszeitungen). So können zum einen Empfehlungen von Freunden oder Menschen mit ähnlichen Interessen für den Leser relevanter sein als die für einen Durchschnittsleser gedachten Empfehlungen eines Experten. Zum Zweiten nutzen Empfehlungen von Menschen mit gleichen Interessen die Wisdom-of-Crowds, um Informationen zu entdecken, die bei den Nutzern beliebt, aber der Aufmerksamkeit der Experten möglicherweise entgangen sind.

Ein Nachteil solcher Empfehlungen ist, dass die Vielfalt an Inhalten, die ein Nutzer erfährt, auf die Inhalte reduziert werden, die Freunde oder Menschen mit gleichen Interessen mögen. Die potenzielle Gefahr hierbei besteht in der Bildung von „Filter Bubbles". Unpopuläre Inhalte (z. B. Nachrichten, die eine unübliche Sichtweise hervorheben) werden herausgefiltert und verschiedene Bevölkerungsgruppen erfahren stark unterschiedliche Inhalte. Dies kann zur Bildung von Untergruppen mit stark divergierenden Weltanschauungen beitragen, da sie sich zu keiner Zeit den Sichtweisen anderer Gruppen gegenübersehen.

Eine Schlüsselherausforderung für die Forschung besteht darin, zu verstehen, wie die Wisdom-of-Crowds genutzt werden kann und wie Empfehlungssysteme entworfen werden können, die interessante und relevante Inhalte identifizieren, ohne dabei die Vielfalt und die Unabhängigkeit der empfohlenen Inhalte zu beeinträchtigen.

NACHRICHTEN, DIE EINE UNÜBLICHE SICHTWEISE HERVORHEBEN, WERDEN HERAUSGEFILTERT UND VERSCHIEDENE BEVÖLKERUNGSGRUPPEN ERFAHREN STARK UNTERSCHIEDLICHE INHALTE. DIES KANN ZUR BILDUNG VON UNTERGRUPPEN MIT STARK DIVERGIERENDEN WELTANSCHAUUNGEN BEITRAGEN, DA SIE SICH ZU KEINER ZEIT DEN SICHTWEISEN ANDERER GRUPPEN GEGENÜBERSEHEN.



3.4 PROBLEMLÖSUNG UND PRODUKTION UNTER VERWENDUNG DES CROWD-SOURCING

Die sozialen Services ermöglichen es den Usern, gleichgesinnte Menschen zu finden und Communitys zu bilden, um gemeinsam an der Lösung komplexer Probleme zu arbeiten

oder um Produkte wie Software oder eine Enzyklopädie zu erstellen. Traditionell wurden solche Aufgaben von ausgewählten Expertengruppen innerhalb eines gut organisierten Umfelds gelöst. Das Crowd-Sourcing stellt einen alternativen Ansatz dar, bei dem Beiträge von Vielen genutzt werden, einschließlich Freiwilliger, die keine Experten sind. Es gibt Probleme, die sich gut für ein Crowd-Sourcing eignen. Dies reicht von der Übersetzung von Texten in verschiedene Sprachen über die Durchsuchung von Satellitenbildern nach Überlebenden in Katastrophengebieten, die Entdeckung besserer Faltungsstrategien für Proteine bis hin zur Meldung von Schlaglöchern in der Nachbarschaft.

Ein effektives Crowd-Sourcing erfordert Anreize für die Nutzer, um Beiträge einzustellen und Online-Communitys zu organisieren, und zwar ohne persönliche Rechenschaft oder etablierte organisatorische Hierarchien. Bestehende Communitys vertrauen auf den Altruismus, auf einen gesunden Wettbewerb unter den Nutzern oder auf eine Bezahlung, um Beiträge zu fördern. Die Organisation basiert auf Vertrauen und der Reputation von Nutzern, die sie durch ihre Beiträge und Leistungen in der Vergangenheit erworben haben.
Die Schlüsselherausforderung in der Forschung liegt darin, das Potenzial und die Grenzen des Crowd-Sourcing zu verstehen sowie zu untersuchen, wie soziale Services zur Bildung und Unterhaltung effektiver Online-Communitys entworfen werden können.

DETAILLIERTE INTERAKTIONSDATEN VON NUTZERN SOZIALER NETZE KÖNNEN VERWENDET WERDEN, UM ZU VERFOLGEN, WIE SICH INFORMATIONEN VERBREITEN – UND DAS IN EINER GRÖSSENORDNUNG UND MIT EINER GENAUIGKEIT, DIE BISHER NICHT DENKBAR WAR.

3.5 RECHNERGESTÜTZTE SOZIALWISSENSCHAFTEN

Soziale Online-Interaktionen können einfach erfasst und protokolliert werden. Die meisten sozialen Netzwerke speichern detaillierte Protokolle der Aktivitäten und Interaktionen Hunderter Millionen einzelner Nutzer auf deren Seiten. Die daraus resultierende große Menge an Daten ist für datengestützte Studien im Bereich der Sozialwissenschaften von unschätzbarem Wert. Dies gilt sowohl hinsichtlich der empirischen Validierung bestehender als auch der Entwicklung neuer Theorien. Die Soziologen haben beispielsweise jahrzehntelang Theorien darüber untersucht, wie sich Informationen in der Gesellschaft verbreiten. Wenige dieser Theorien konnten jedoch in großem Maßstab empirisch validiert werden, da nur schwer zu erfassen ist, wie sich Informationen in der realen Welt verbreiten. Im Gegensatz dazu können detaillierte Interaktionsdaten von Nutzern sozialer Netze verwendet werden, um zu verfolgen, wie sich Informationen verbreiten – und das in einer Größenordnung und mit einer Genauigkeit, die bisher nicht denkbar war.

Die Schlüsselherausforderungen in der Forschung liegen in der Analyse großer Datenmengen, um neue Erkenntnisse über soziale Interaktionen zwischen Usern zu gewinnen. Gleichwohl muss der Datenschutz und die Privatsphäre der Nutzer respektiert und die Unterschiede zwischen sozialen Interaktionen in der Online- und der Offlinewelt berücksichtigt werden.

3.6 DATENSCHUTZ IM INTERNET

Da die Nutzer ihre persönlichen Informationen, sozialen Beziehungen, viele ihrer alltäglichen Aktivitäten und ihre Aufenthaltsorte in sozialen Online-Services offenlegen, ist der Datenschutz von außerordentlichem Belang. Es gibt drei Hauptgefahren in Bezug auf den Datenschutz:

Eine großzügige Offenlegung persönlicher Informationen: OSN-Teilnehmer neigen dazu, persönliche Informationen offenzulegen, sowohl explizit als Teil ihrer Angaben zur Person und durch die Beschreibungen ihrer täglichen Aktivitäten (Textbeiträge, Fotos und Videos), als auch implizit durch Informationen, die durch ihre persönlichen mobilen Geräte erfasst werden (z. B. über den Standort). Viele Nutzer ziehen die kurz- und langfristigen Folgen der Offenlegung dieser persönlichen Informationen nur unzureichend in Betracht. Zudem kann eine Offenlegung von Informationen im Allgemeinen nicht rückgängig gemacht werden. Selbst wenn ein Nutzer Informationen löscht, ist es in einem offenen System wie dem Internet nicht möglich, sämtliche Kopien zu lokalisieren und zu löschen, die dritte Parteien gemacht haben könnten, solange die Information öffentlich war.

Mangelndes Verständnis der Datenschutzeinstellungen: Viele OSN-Teilnehmer sind sich der Auswirkungen ihrer gewählten Datenschutzeinstellungen nicht bewusst und viele ändern die vom Dienstleiter gewählten Einstellungen erst gar nicht. Folglich sind sich Nutzer oft nicht darüber im Klaren, wer in der Lage ist, ihre Informationen zu sehen. Dies führt nicht selten zu peinlichen Vorfällen, weil sich die Nutzer nicht bewusst sind, dass die Familie oder der Vorgesetzte in der

Lage ist, bestimmte Informationen zu sehen. Dies kann unter Umständen Folgen für deren Ehe, Karriere oder soziales Ansehen nach sich ziehen.

Unwissenheit über implizite „Löcher" in der Privatsphäre: Selbst Internetuser, die für die Datenschutzproblematik sensibilisiert sind, sind sich oft nicht im Klaren darüber, wie viele ihrer persönlichen Informationen durch Data-Mining und statistische Methoden rekonstruiert werden können, und zwar aus kleinsten Informationen, die bei der Nutzung verschiedener Onlinedienste preisgegeben werden. Durch das Abgleichen von Surf- und Suchaktivitäten mit anderen öffentlichen Informationen aus dem Web ist es oft möglich, mit hoher Sicherheit auf den Namen des Internetusers, seine Altersgruppe, seine Gehaltsklasse, seinen ungefähren Wohnort oder den Standort des Büros, seine politischen Ansichten, seinen religiösen Glauben, seinen Familienstand, seine Hobbys, Interessen und sogar auf seine sexuelle Orientierung zu schließen. Dies ist sogar dann möglich, wenn der Nutzer nicht in OSNs oder Tauschbörsen partizipiert und seine Informationen nicht in anderer Form explizit offenlegt.

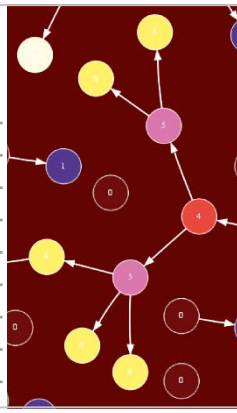
Eine Preisgabe persönlicher Daten kann darüber hinaus Auswirkungen für die persönliche Sicherheit des Nutzers haben. Die Website pleaserobme.com will das Bewusstsein hinsichtlich eines Aspekts dieser Gefahr fördern, in dem sie Informationen von Twitter (wo die Nutzer ihren gegenwärtigen Aufenthaltsort bekannt geben) und Foursquare (wo Nutzer ihre Wohnanschrift offenlegen) kombiniert, um so anzuzeigen, wann ein Haus gerade nicht beaufsichtigt wird und somit ein attraktives Ziel für einen Einbruch darstellt. In anderen Fällen erfasst ein Angreifer genügend persönliche Informationen über ein Opfer, um dessen Bank anzurufen und sich dort erfolgreich als das Opfer auszugeben und die Bank zu bitten, Geld zu überweisen.

Eine Schlüsselherausforderung in der Forschung ist die Entwicklung von Prinzipien, Modellen und Mechanismen für den Online-Datenschutz, welche unbedarften Nutzern adäquate Kontrollmöglichkeiten über ihre persönlichen Daten an die Hand geben und es ihnen ermöglichen, sich hinsichtlich ihrer Datenschutzeinstellungen informiert entscheiden zu können.

3.7 ONLINE-IDENTITÄT UND RECHENSCHAFT

Die Identität von Nutzern stellt einen Schlüsselaspekt bei allen sozialen Onlinesystemen dar. Um möglichst viele Nutzer zu gewinnen, verlangen die Online-Services wenn überhaupt nur wenige Anmeldedaten von Nutzern, um einen Account und eine entsprechende Identität anlegen zu können. Daher können Nutzer unter fiktiven Namen handeln, ihr Geschlecht, ihr Alter oder ihr Erscheinungsbild verfälschen, die Identität einer anderen Person oder sogar mehrere Identitäten annehmen, oder innerhalb mehrerer Identitäten wechseln, um einer schlechten Reputation zu entgehen. Dieser Mangel an vertrauenswürdigen Identitäten führt zu Angriffen sowohl auf der persönlichen wie auch auf der organisatorischen Ebene. Manche Nutzer verwenden falsche Identitäten, um auf Auktionsseiten wie eBay zu betrügen, um Diskussionen in Chatrooms zu stören, um andere Nutzer anonym zu verleumden oder um Wikipedia-Einträge zu verunstalten. Ein pädophiler Mensch kann, indem er vorgibt, gleichaltrig zu sein, Kontakte zu Kindern aufbauen und deren Vertrauen gewinnen. Organisationen können viele falsche Identitäten erstellen, um die öffentliche Meinung hinsichtlich geschäftlicher oder politischer Ziele zu beeinflussen.

DURCH DAS ABGLEICHEN VON SURF- UND SUCHAKTIVITÄTEN IST ES OFT MÖGLICH, MIT HOHER SICHERHEIT AUF DEN NAMEN DES INTERNETUSERS, SEINE ALTERSGRUPPE, SEINE GEHALTSKLASSE, SEINEN UNGEFÄHREN WOHNORT ODER DEN STANDORT DES BÜROS, SEINE POLITISCHEN ANSICHTEN, SEINEN RELIGIÖSEN GLAUBEN, SEINEN FAMILIENSTAND, SEINE HOBBYS, INTERESSEN UND SOGAR AUF SEINE SEXUELLE ORIENTIERUNG ZU SCHLIESSEN.



Gleichzeitig besteht jedoch auch ein legitimer Bedarf an Anonymität in den sozialen Onlinesystemen. Sie spielen eine wichtige Rolle als Plattformen für Redefreiheit, für eine unabhängige Berichterstattung und als Basis für politischen Aktivismus. Während Nutzer oft davon ausgehen, anonym zu sein, haben Regierungen und Geheimdienste oftmals die technischen Mittel, um die Identität von Nutzern aufzudecken, wodurch sie in der Lage sind, Informanten, Regimekritiker oder die politische Opposition zu verfolgen.

Eine Schlüsselherausforderung liegt darin, die Grundlagen von Identität, Anonymität und der Rechenschaft in sozialen Onlinesystemen zu erforschen und rechtliche und technische Mechanismen zu entwickeln, die den widersprüchlichen Bedürfnissen der persönlichen Rechenschaft einerseits und der legitimen Anonymität andererseits gerecht werden.

ORGANISATIONEN KÖNNEN VIELE FALSCHE IDENTITÄTEN ERSTELLEN, UM DIE ÖFFENTLICHE MEINUNG HINSICHTLICH GESCHÄFTLICHER ODER POLITISCHER ZIELE ZU BEEINFLUSSEN. GLEICHZEITIG BESTEHT JEDOCH AUCH EIN LEGITIMER BEDARF AN ANONYMITÄT IN DEN SOZIALEN ONLINESYSTEMEN. SIE SPIELEN EINE WICHTIGE ROLLE ALS PLATTFORMEN FÜR REDEFREIHEIT, FÜR EINE UNABHÄNGIGE BERICHTERSTATTUNG UND ALS BASIS FÜR POLITISCHEN AKTIVISMUS.

3.8 WIRTSCHAFTLICHE UND RECHTLICHE RAHMENBEDINGUNGEN FÜR DIE NUTZUNG VON ONLINE-DATEN

Während die Nutzer immer mehr ihrer persönlichen Daten online speichern und veröffentlichen, sind die wirtschaftlichen und rechtlichen Rahmenbedingungen, die deren Nutzung abdecken, nach wie vor nicht adäquat. Die Anbieter sozialer Onlinedienste behalten sich oftmals das unbeschränkte Recht vor, Nutzerdaten zu speichern und diese zu verwenden. Die meisten Firmen bieten ihre Dienstleistungen kostenlos an und hoffen im Gegenzug, die persönlichen Daten der Nutzer kommerziell zu verwenden, zum Beispiel für gezielte Werbung. Während die Anbieter sozialer Services verschiedene wirtschaftliche Modelle und Wege erproben, um Erträge aus den persönlichen Daten der Nutzer zu erzielen, gibt es derzeit noch wenig wirksamen rechtlichen Schutz gegen einen Missbrauch von Online-Daten. So ist zum Beispiel in mehreren Ländern unklar, welche rechtlichen Maßgaben einen Krankenversicherer daran hindern, die Beiträge in einem sozialen Onlinedienst zu analysieren, um Informationen über die medizinische Vorgeschichte eines Antragstellers zu erhalten, auch wenn es ihm rechtlich nicht gestattet gewesen wäre, diese direkt vom Antragsteller anzufordern.

Auf der anderen Seite müssen Regierungen und Aufsichtsbehörden, wenn sie neue Gesetze und Vorschriften zum Schutz von Online-Daten in Betracht ziehen, ebenfalls den Einfluss auf das Wachstum und die Innovation in der Online-Wirtschaft berücksichtigen. Während legislative Bemühungen der Regierungen dabei helfen können, Verbraucher zu schützen, kann eine unsinnige oder übersteigerte Gesetzgebung wirtschaftliches Wachstum und Innovation behindern.

Die Forschungsherausforderung hierbei ist es, geeignete wirtschaftliche und rechtliche Rahmenbedingungen für die Nutzung von Online-Daten zu entwickeln, die die Verbraucher schützen, und gleichzeitig wirtschaftliches Wachstum und Innovation ermöglichen. Ebenso sollten Gesetzgeber und Industrie entsprechend beraten werden.

4. PERSPEKTIVE UND ERGEBNISSE

Eine stark interdisziplinäre Gemeinschaft von Wissenschaftlern im Bereich des Social Computing ist im Entstehen, in der Wissenschaftler der Bereiche Informatik, Wirtschaftswissenschaft, Sozialwissenschaften und Rechtswissenschaften arbeiten, die über beträchtliches Wissen in einer oder mehrerer der anderen Disziplinen verfügen. Darüber hinaus haben mehrere amerikanische Universitäten Programme in Information Science etabliert, die sich auf eine interdisziplinäre Ausbildung im Bereich Informatik in Verbindung mit Sozialwissenschaft, Politikwissenschaft, Psychologie, Rechtswissenschaften und Wirtschaftswissenschaften konzentrieren.

Die Informatik spielt in der Forschung über Social Computing eine zentrale Rolle, da sie über zahlreiche wesentliche Methoden verfügt: die Analyse großer Mengen von Daten über Online-Interaktionen, statistische Techniken zur Bestimmung des Grads, mit dem sich private Informationen aus individuellen Daten ableiten lassen, den Entwurf mathematischer Logiken und formaler Sprachen zur Spezifizierung, die Analyse und Erzwingung von Datenschutzeinstellungen, den Entwurf kryptografischer Techniken für den Datenschutz, der Sicherheit und Rechenschaft, die Entwicklung von Datenschutzmodellen und Kontrollen, die auch unbedarfte Nutzer verstehen und nutzen können, und die Erstellung von Software, die entwurfsbedingt Sicherheit und Datenschutz gewährleistet.

Faktisch kann jedoch keine der wichtigen Forschungsherausforderungen im Bereich des Social Computing nur mit den Methoden der Informatik allein untersucht werden. Sie erfordern gemeinsame Bemühungen sowohl der Informatiker als auch der Sozialwissenschaftler, der Juristen und der Wirtschaftswissenschaftler. In Zukunft wird voraussichtlich eine Generation von Forschern im Bereich des Social Computing entstehen, deren Ausbildung die Grenzen dieser Disziplinen überschreitet.

Referenzen

[1] D. Easley und J. Kleinberg. Networks, Crowds, and Markets: Reasoning About a Highly Connected World. Cambridge University Press, 2010.

[2] R. Kraut und P. Resnick. Building Successful Online Communities: Evidence-based Social Design. MIT Press, 2012.

[3] B. Krishnamurthy. I know what you will do next summer. Computer Communications Review, 40, 2010.

[4] D. J. Watts. A twenty-first century science. Nature, 445, August 2007.

KRISHNA GUMMADI, PETER DRUSCHEL, PAUL FRANCIS
MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS, KAISERSLAUTERN AND SAARBRÜCKEN

Social Computing

1. INTRODUCTION

During the Arab Spring, Twitter and Facebook played a significant role in spreading information and organizing protesters. Justin Bieber became a teen singing sensation after posting videos of himself on Youtube. Anybody can post reviews on sites like Amazon and Netflix, thereby helping complete strangers make informed decisions about what to buy. In the US, social media are used to organize "flash robs", where large groups of people converge on a shop and steal goods. These examples clearly show the impact information technology and social media are having on society.

Social Computing is an emerging area of research, which studies these and other phenomena that arise when people interact, collaborate and compete by means of information technology. These types of social interactions mediated by information technology are at the core of today's Internet, which has emerged as a global multimedia platform for communication, social networking, entertainment, education, information, self-expression, trade, and political activism.

During the past decade, we have entered what can be termed the "social computing era". Compared to the early Internet, today's Internet users are no longer passive consumers of information and services provided by professional information sources and service providers. Instead, today's users actively publish multimedia content in sharing services like YouTube, participate in social networks like Facebook, and trade goods and services in online auction houses like eBay. They share opinions and experiences with products on shopping and booking sites, contribute their knowledge and expertise in blogs and Wikipedia, spread ideas over Twitter, and sell their freelance services in work marketplaces like Mechanical Turk. In effect, the modern Internet leverages information technology to provide a virtual platform on which people engage in the full range of social activity.

The social computing era, however, also brings with it new threats. The unprecedented amount of information captured about individuals' actions and preferences can be used for nefarious purposes. Personalized information services that cater to individuals' known interests can lead to "filter bubbles", in which users are rarely exposed to information that could widen their perspective or challenge their world view. And, people are relying increasingly on online social discourse, possibly at the expense of offline social interactions.

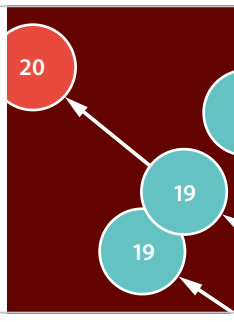
The popularity of social services, amplified by the proliferation of smart phones, other mobile devices and ubiquitous Internet access in large parts of the world, have had a profound impact on the global economy and the very fabric of society:

Social relationships Information technology enables and supports online communities, which have the potential to enhance individuals' quality of life, increase society's productivity, and democratize information exchange and political discourse. Social computing research studies the organization and evolution of online communitites, and the principles underlying the design of social services that can leverage online communities effectively.

Information dissemination Online users increasingly take cues from each other instead of relying on traditional authorities like media outlets, corporations, government, political parties and religious organizations for information and guidance. Social computing research seeks to study the principles and mechanisms by which information flows, opinion spreads, and individuals are influenced in the online world.

New threats Social information technologies raise serious concerns about individuals' privacy, security, and freedom, and create new avenues for manipulation and misinformation, filter bubbles, the potential for social isolation in the real world and the widening of the digital divide. Social computing research seeks to understand these threats, and study social, technological, legal and economic responses to mitigate them.

PERSONALIZED INFORMATION SERVICES THAT CATER TO INDIVIDUALS' KNOWN INTERESTS CAN LEAD TO "FILTER BUBBLES", IN WHICH USERS ARE RARELY EXPOSED TO INFORMATION THAT COULD WIDEN THEIR PERSPECTIVE OR CHALLENGE THEIR WORLD VIEW.



Thus, social computing, in its broad sense, studies the opportunities and challenges that arise when human social activity is augmented and transformed by information technology. This emerging interdisciplinary field intersects computer science, social science, law and economics. Some of the key phenomena studied include social networking, content sharing, and blogging; social peer production and crowd sourcing; massive multi-player games and virtual

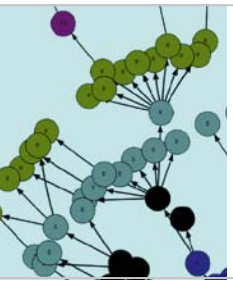
worlds for entertainment and training; online commerce, auctions and advertising; online privacy and accountability, spam and cybercrime.

Network science is a related interdisciplinary field (involving computer scientists, physicists, mathematicians and researchers from other disciplines), which is focused on the study of physical, biological, technical and social phenomena that can be modeled as complex graphs or networks. The field intersects with social computing in its study of social networks. Here, network science is focused on the graph properties of social networks, while social computing considers the full range of technical, economic and social aspects of these and other systems.

In this article, we give an overview of the key challenges and opportunities in the emerging field of social computing from the perspectives of individuals, industry, and society, as well as future directions in this exciting interdisciplinary field. It is important to note that social computing spans multiple research fields and it is still in its infancy. As a result, researchers from different fields hold different perspectives on what the key questions and challenges are, and how the field will evolve. This article largely reflects the authors' perspective as computer scientists.

2. BACKGROUND

We start with a brief description of some of the most popular social systems and services in today's Internet, in order to provide background for our discussion of the key challenges and opportunities in social computing.



SOCIAL COMPUTING IS AN EMERGING AREA OF RESEARCH, WHICH STUDIES PHENOMENA THAT ARISE WHEN PEOPLE INTERACT, COLLABORATE AND COMPETE BY MEANS OF INFORMATION TECHNOLOGY.

2.1 ONLINE SOCIAL NETWORKS AND CONTENT SHARING

Online social networks (OSN) like Facebook and its numerous more specialized or regional competitiors are among the most popular online services today. Facebook alone claims to have 845 million users, as of December 2011. OSNs allow users to declare who their friends and colleagues are, and browse the resulting social network. They allow users to share information about themselves and their activities with friends, friends of friends, and the general public. OSNs exacerbate the conflicting human desires to both share information and maintain privacy, often causing users to expose sensitive information in unintended and damaging ways.

Content sharing sites like YouTube allows users to share their videos with friends and the public. These videos may be produced by the users themselves (often representing original creative works, newsworthy footage, or "how to" instructions) or by others. Users can recommend videos, and use these recommendations to find videos they may like. This results in certain videos going "viral", allowing everyday users to create and publish videos seen by millions and even become online celebrities.

2.2 BLOGS AND MICROBLOGS

Blogs (short for web logs) are a form of personal online diary, which allows the owner to share information and musings about their lives or a specific subject with the interested public, or with a set of online friends. Blogs by celebritites, politicians and domain experts are highly popular and in many cases followed by millions of people. Twitter provides a micro-blog service, where users can publish frequent short text messages called tweets from their mobile phones, which are then distributed in real-time to the user's followers, a set of people who have registered to receive the user's tweets. Twitter has over 100 million active users and distributes more than 230 million tweets per day, as of September 2011.

2.3 ONLINE COMMERCE: SHOPPING AND AUCTIONS

Online shopping sites like Amazon offer a wide variety of products for purchase. In addition to conventional product descriptions, users have access to recommendations and reviews from users who have previously purchased a product. Moreover, Amazon mines users' browsing and purchasing behavior, in order to suggest products a user might be interested in. Online auction sites like eBay allow users to offer their own goods and bid on other users' offerings. Based on feedback from users, the system keeps track of seller and buyer reputations, in order to warn users of potential fraud. E-commerce sites have become enormously popular, with online product sales estimated at 142.5 billion US dollars, accounting for 8% of all US retail sales in 2011. Further, online sales are estimated to double by 2015.

2.4 PEER-PRODUCTION AND CROWD-SOURCED SYSTEMS

Wikipedia is an example of a social peer production system. It provides an online encyclopedia that relies entirely on volunteers to write, edit and curate its entries. Most entries can be edited by any user, but volunteer editors responsible for a given entry review and approve changes and new material. Editors are often known under an online pseudonym only; they are trusted by the community based on their past performance rather than any formal credentials. Charitable contributions are solicited from users to cover the cost of operating the technical infrastructure that provides the service.

Another example of a peer production system is Mechanical Turk, an online marketplace for work. It provides businesses, developers and scientists with an on-demand, scalable workforce, by matching so-called human intelligence tasks (HITs) with online users who are willing to perform these tasks for money. A typical task is to label photographs with keywords that best describe their content. This task is easy for humans but very difficult for today's computers to perform. Mechanical Turk combines the strengths of information technology (managing large amounts of task data, matching tasks with labour wherever in the world it is available) with human skill and ability.

2.5 ONLINE ADVERTISING

A significant proportion of services in the Internet are free for users. The companies offering these services (including Facebook, Google, Yahoo, etc.) generate revenue by selling advertisements. Online ads achieve high prices in the advertising industry, partly because users spend a lot of time online, partly because ads can be targeted based on a user's present activity (e.g., search queries) or past behavior. For the purposes of targeted advertising, aggregators and search engines like Google and Bing produce profiles of users based on their history of search queries and web site visits, web email providers like Gmail and HotMail mine the contents of user emails, and OSNs like Facebook mine the personal information provided by their users.

3. KEY RESEARCH CHALLENGES

In this section, we discuss some of the fundamental questions and key research challenges raised by the social systems and services discussed in the previous section.

3.1 ONLINE SOCIAL TIES AND ONLINE EXPOSURE

Social computing technologies have made it easy for people to communicate, bond, and share information with their social groups across physical distances. Through social networking sites like Facebook, users can keep in touch with family and friends, and find and reconnect with old friends and coworkers. These sites facilitate online interactions by way of sharing status updates and content, which reinforces social structures and helps people to bond, build, and maintain relationships across distances.

FACEBOOK HAS 845 MILLION USERS. TWITTER HAS OVER 100 MILLION ACTIVE USERS AND DISTRIBUTES MORE THAN 230 MILLIONS TWEETS PER DAY, AS OF SEPTEMBER 2011. E-COMMERCE SITES HAVE BECOME ENORMOUSLY POPULAR, WITH ONLINE PRODUCT SALES ESTIMATED AT 8% OF ALL US RETAIL SALES IN 2011. FURTHER, ONLINE SALES ARE ESTIMATED TO DOUBLE BY 2015.

However, the extensive use of online social services, especially by younger generations, may come at a cost to their offline (real-world) social interactions. In fact, the popularity of online social interactions seems to change prevalent social norms on how people interact with one another and what information people share with whom. While one can debate the relative merits of online and offline social norms, users may be more comfortable expressing their opinions and sharing their personal information publicly in the online world than they are in the offline world. A lot of the content shared on the social sites is personal, multi-media content, e.g., photos and videos of family vacations or office parties. Furthermore, the content is often widely accessible, raising severe privacy concerns and amplifying the impact of social misbehaviors like bullying, slander, and stalking.

A key research challenge is to understand how online social services affect the social fabric of online and offline relationships, and how the sharing of personal online information both violates and changes social norms about privacy.

3.2 THE DEMOCRATIZATION OF PUBLISHING AND WORD-OF-MOUTH PROPAGATION

The low storage and transmission cost of digital data has enabled content sharing sites like YouTube, which have in turn democratized content publishing. By lowering the barriers for publishing, YouTube has attracted contributions from millions of users worldwide on topics ranging from creative performances to news accounts to discussions of specialized sub-

jects like quantum physics. Users creating the videos express opinions that range from the mundane (discussions about TV shows) to the educational (guitar-playing lessons) to the political (calling for revolt against established authorities).

Furthermore, the content published by ordinary users can be disseminated by other users by "word-of-mouth". Everyday users share hundreds of millions of URLs (links to webpages, blogs, and YouTube videos) that they discover with their friends and followers over Facebook and Twitter. Thus, social computing technologies democratize content publishing and dissemination by allowing any user to post content they generate on social networking sites and have it spread to other users by word-of-mouth.

A key research challenge here is to understand the dynamics of word-of-mouth propagation, how to distinguish rumors and lies from true stories, and how to ascertain the trustworthiness of a source. This understanding is criticial to our ability to design social systems that can deliver relevant and trustworthy information.

3.3 LEVERAGING THE WISDOM-OF-CROWDS TO FIND RELEVANT INFORMATION

Social services can leverage the wisdom-of-crowds (that is, user feedback) to find information relevant to a user. For example, user ratings of YouTube videos are used to rank the search results for YouTube videos. Similarly, the Amazon shopping site recommends books to a user based on what books the user previously bought and what other users who bought the book also bought and liked.

Content recommendations from peers differ from traditional content selection by a small number of well-known authorities (e.g., newspaper editors) in some important ways. First, content recommended by peers who are known friends or who have similar interests may be more relevant to a reader than content recommended by an authority for a generic reader. Second, peer recommendations leverage the wisdom-of-the-crowds to discover information that is popular with ordinary users but might escape the attention of experts.

One downside with such content recommendations by peers is that the diversity of content that a user is exposed to might be curtailed as the user is only presented content that his friends or peers might like. The potential danger here is the creation of "filter bubbles", where certain content (e.g., news stories highlighting a perspective different from that of one's peers) is filtered out or where different groups of users in the population are exposed to radically different content. Filter bubbles can contribute to the formation of sub-groups of users with increasingly divergent world-views, as they are never exposed to the views of other groups.

Here, a key research challenge is to understand how to leverage the wisdom-of-crowds, and how to design peer recommendation systems that identify interesting and relevant content, while not compromising on the diversity and independence of the recommended content.

3.4 PROBLEM SOLVING AND PRODUCTION USING CROWD-SOURCING

Social services enable users to seek out like-minded people and form communities to collaboratively work towards solving complex problems or produce artifacts like software or an encyplopedia. Traditionally, such problems have been tackled by select groups of experts within a well-organized setting. Crowd-sourcing represents an alternative approach where contributions are leveraged from crowds, including potentially non-expert volunteers. Some problems are well suited for crowd-sourcing, ranging from translating text between languages and searching satellite images to rescuing people in disaster areas to discovering better protein folding strategies and reporting about neighborhood potholes.

Effective crowd-sourcing requires incentives for users to contribute, and ways to organize online communities in the absence of strong personal accountability or established organizational hierarchies. Existing communities rely on atruism, users' competitive spirit, or payment to encourage contributions, and the organization is based on trust and reputation grounded in past contributions and performance.

The key research challenge lies in understanding the potential and limitations of crowd-sourcing, and how to design social services that can support the formation and maintentance of effective online communities.

3.5 COMPUTATIONAL SOCIAL SCIENCE

Online societal interactions are easy to capture and record. Most social networking sites keep detailed records of the activities of hundreds of millions of individual users on their sites, including the interactions between them. The resulting abundance of data is invaluable for data-driven studies in social science, both to empirically validate existing theories and to develop new theories. For example, for decades, sociologists have studied theories of how information propagates in a society. However, few of the theories have been empirically

validated at scale, as it is hard to capture how a piece of information spreads in an offline world. In contrast, detailed data about user interactions from social networking sites can be used to track how information diffuses in a network at a scale and granularity that was previously inconceivable.

The key research challenges lie in analyzing large volumes of data to derive new insights about societal interactions between users, while respecting the privacy of users whose data is being analyzed, and considering the differences between online and offline social interactions.

3.6 ONLINE PRIVACY

Of major concern is privacy, given that users expose their personal information, social relationships, and much of their day-to-day activity and whereabouts in online social services. There are three main threats to privacy:

Liberal disclosure of personal information: OSN participants tend to disclose personal information, either explicitly as part of their profile and by reporting on their daily activities using text, photos and videos, or implicitly through information captured by their personal mobile devices (e.g., location). Many users fail to fully consider the short and long-term consequences of disclosing personal information. Moreover, public disclosure is generally irreversible: even if a user subsequently removes information, it is impossible in an open system like the Internet to locate and delete all copies that third parties might have made while the information was public.

Failure to understand privacy controls: OSN participants tend to be unaware of the effects of their privacy settings, and many user never change the default settings chosen by the provider. As a result, they tend to be unaware of who is permitted to see their information. This leads to frequent cases of public embarrassement, because users were not aware that their family or supervisor are able to see certain information, with potential consequences for their marriage, career, or social reputation.

Unawareness of implicit privacy leaks: Even privacy-conscious Internet users tend to be unaware of how much of their personal information can be obtained through data mining and statistical inference based on small amounts of trace data they leave while using different online services. By correlating the browsing and searching activity with public information on the Web, it is possible to infer with high confidence an Internet user's name, age bracket, income bracket, approximate residential and office location, political views, religious faith, family status, hobbies, interests and even sexual orientation. This information can often be obtained even if the user does not participate in OSNs or sharing sites, and does not otherwise explicitly disclose this information.

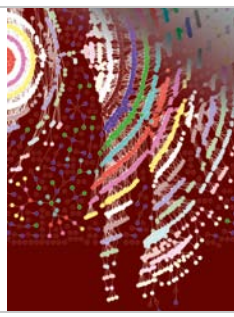
Leakage of personal data can also have implications for users' personal security. The web site pleaserobme.com seeks to raise awareness about one aspect of this threat by combining information from Twitter (in which people announce their current whereabouts) and foursquare (where people disclose their residential address) to announce when a home is unattended and thus an attractive target to rob. In other cases, an attacker gathers enough personal information about a victim online to call their bank and successfully pose as the victim and ask for money to be transfered.

A key research challenge is the development of principles, models, and mechanisms for online privacy that give lay users adequate controls over privacy, and allow them to make informed privacy choices.

3.7 ONLINE IDENTITY AND ACCOUNTABILITY

A core aspect of all online social systems is that of user identity. In order to attract a large number of users, most online services require few if any credentials to create an account and corresponding identity. As a result, individuals can act under fictitious names, lie about their gender, age, or appearance, falsely assume the identity of a real person, assume multiple identities, or switch identities to escape a bad reputation. This lack of trusted identities leads to attacks at both the individual and organizational level. Individuals frequently exploit weak identities to commit fraud in auction sites like eBay, disrupt online bulletin boards, commit anonymous slander in OSNs, or deface Wikipedia entries. A pedophile can establish contact and earn the trust of children by posing as a same-aged peer. And organizations can create many false identities to sway public opinion for commercial or political ends.

WHILE ONE CAN DEBATE THE RELATIVE MERITS OF ONLINE AND OFFLINE SOCIAL NORMS, USERS MAY BE MORE COMFORTABLE EXPRESSING THEIR OPINIONS AND SHARING THEIR PERSONAL INFORMATION PUBLICLY IN THE ONLINE WORLD THAN THEY ARE IN THE OFFLINE WORLD.



At the same time, there is a legitimate need for anonymity in online social systems. Today's online services play an important role as a platform for free speech, independent reporting, and grassroots political activism. While users may believe themselves to be anonymous, governments or intelligence organizations often have technical means to discover user identities, allowing them to repress whistleblowers, dissidents, or political opposition.

A key challenge is to understand the principles of identity, privacy and accountability in online social systems, and to create legal and technical mechanisms that balance the conflicting needs of holding users accountable for misbehavior and allowing users to remain anonymous where appropriate.

3.8 ECONOMIC AND LEGAL FRAMEWORKS GOVERNING ONLINE DATA

Even as users store and publish more and more of their personal data online, the current economic and legal frameworks governing their usage remain inadequate. Companies offering social services often retain unrestricted rights to store and use any data uploaded by users of their services. Most companies offer their services for free and in return they hope to gather and exploit users' personal data, for example to target advertisements personalized for the user. As companies providing social services try various economic models and ways to generate revenues from users' personal data, there are few effective legal protections against misuse of online data. For instance, in several countries, it is unclear what legal provisions prevent a health insurance provider from analyzing an applicant's posts on a social site to obtain information about pre-existing medical conditions of the applicant that they are legally not allowed to request directly from the applicant.

DETAILED DATA ABOUT USER INTERACTIONS FROM SOCIAL NETWORKING SITES CAN BE USED TO TRACK HOW INFORMATION DIFFUSES IN A NETWORK AT A SCALE AND GRANULARITY THAT WAS PREVIOUSLY INCONCEIVABLE.

On the other hand, as governments and regulators worldwide consider new laws and regulations to safeguard online data, they need to consider the impact on growth and innovation in the online economy. While legislative efforts by governments can help protect consumers, misguided or overreaching legislation can hamper economic growth and innovation.

The research challenge here is to develop appropriate economic and legal frameworks governing online data that protect consumers yet allow economic growth and innovation, and to consult legislators and industry accordingly.

4. OUTLOOK AND CONCLUSIONS

A truly interdisciplinary community of social computing researchers is developing, in which researchers are primarily trained in computer science, economics, social sciences, or law, but have substantial background in one or more of the other disciplines. Moreover, several US universities have established programs and schools in information science, which are focused on providing interdisciplinary training in computer science and one or more of social science, political science, public policy, psychology, law and economics.

Computer science will play a central role in the social computing research endeavor, through methods like large-scale data analysis of online interactions, statistical techniques to determine how much private information can be inferred from individual data items, design of mathematical logics and formal languages to specify, reason about and enforce privacy choices, design of cryptographic techniques for privacy, security and accountability, design of privacy models and controls that can be understood and reasoned about by lay users, and the design of software architectures that maintain safety and privacy by design. Virtually none of the important research challenges in social computing, however, can be studied with computer science methods alone. They require collaborative efforts between computer scientists and researchers in the social sciences, law or economics. In the future, a generation of social computing scholars will likely emerge whose training crosses the boundaries of these disciplines.

References

[1] D. Easley and J. Kleinberg. Networks, Crowds, and Markets: Reasoning About a Highly Connected World. Cambridge University Press, 2010.

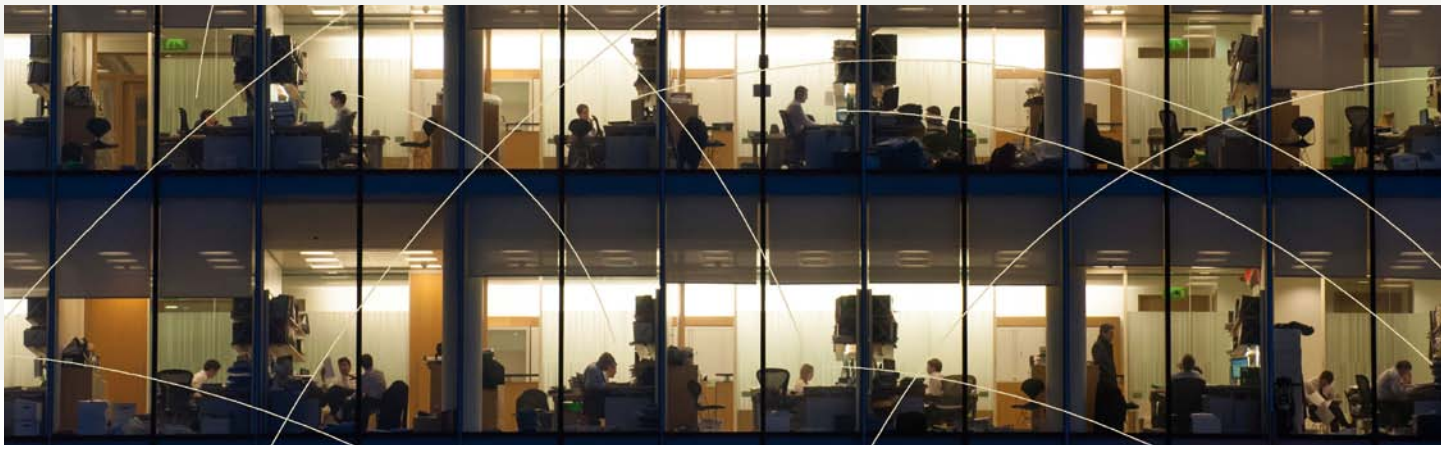
[2] R. Kraut and P. Resnick. Building Successful Online Communities: Evidence-based Social Design. MIT Press, 2012.

[3] B. Krishnamurthy. I know what you will do next summer. Computer Communications Review, 40, 2010.

[4] D. J. Watts. A twenty-first century science. Nature, 445, August 2007.

PROF. DR. DR. H.C. MULT. ULRICH SIEBER
MAX-PLANCK-INSTITUT FÜR AUSLÄNDISCHES UND INTERNATIONALES STRAFRECHT, FREIBURG I.BR.

Cybercrime und Strafrecht in der globalen Informationsgesellschaft



Das Freiburger Max-Planck-Institut für ausländisches und internationales Strafrecht analysiert in seinem strafrechtlichen Forschungsprogramm die Veränderungen von Kriminalität und Strafrecht in der globalen Informations- und Risikogesellschaft. Schwerpunkte sind Terrorismus, Völkerstraftaten, organisierte Kriminalität, Wirtschaftskriminalität und Computerkriminalität. Das hier dargestellte Teilprojekt „Cybercrime und Strafrecht der Informationsgesellschaft" untersucht mit empirischen, strafrechtsvergleichenden und dogmatischen Methoden den Wandel der Informationstechnik, der Kriminalität und des Rechts in der modernen Informations- und Netzwerkgesellschaft. Ziel ist die Analyse der einschlägigen Delikte und ihrer – nationalen und internationalen – Regelungen sowie die Entwicklung von neuen kriminalpolitischen Konzepten, mit denen auf die neuen Herausforderungen reagiert werden kann. Die Einbeziehung der theoretischen Grundlagen des Informationsstrafrechts trägt dabei zur Entwicklung anwendungsorientierter Lösungen bei, die der immateriellen Natur von Daten, dem globalen Charakter des Cyberspace und der Anonymität im Internet Rechnung tragen.

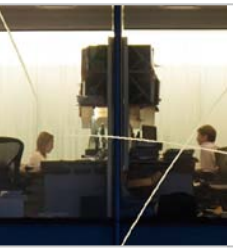
VERLETZLICHKEIT DER INFORMATIONSGESELLSCHAFT

Straftaten im Internet stellen ein existentielles Risiko für die moderne Informationsgesellschaft dar. Zentrale Bedrohungen sind dabei Angriffe gegen die Integrität von Computersystemen, insbesondere Hacking, Manipulation und Zerstörung von Daten sowie die Verbreitung von Schadsoftware und unberechtigtes Erlangen von Zugangsdaten. Diese Delikte gefährden elementare Grundlagen der Wirtschaft, der Verwaltung und des privaten Sektors, die von einer sicheren Datenverarbeitung und Datenkommunikation abhängen. Die Verlässlichkeit von Informations- und Kommunikationssystemen ist besonders bedroht, da diese wegen konzeptioneller Schwächen der eingesetzten Computersoftware sowie der Nachlässigkeit ihrer Nutzer oft nicht ausreichend gesichert sind. Die informationstechnische Infrastruktur der modernen Gesellschaft kann daher in besonderem Maße von weltweit agierenden Tätern über das Internet angegriffen werden. Dies gilt für die Computer von Unternehmen, die Informationstechnik im öffentlichen Sektor und den PC eines jeden Internetbenutzers. Es betrifft Computersysteme von Banken, Produktionsunternehmen, Verwaltung und Militär genauso wie die von Kernkraftwerken, Krankenhäusern und Flugzeugen.

In ähnlicher Weise führen illegale Inhalte im Internet zu erheblichen Risiken: Daten können im Cyberspace schnell, massenhaft und weltweit verbreitet werden, ohne dass eine wirksame nationalstaatliche Kontrolle möglich ist. Auch der Zugriff auf Kinderpornografie wird durch die Kommunikationsmöglichkeiten und die Anonymität des Internets erheblich erleichtert. Die Kontrollprobleme von Daten zeigen sich aber auch bei massenhaft begangenen Urheberrechtsverletzungen, beim grenzüberschreitenden Glücksspiel sowie beim illegalen Vertrieb von Produkten, bei terroristischer oder bei extremistischer Werbung im Internet.

Das große Volumen der von Staat und Wirtschaft gespeicherten personenbezogenen Daten, ihr hoher kommerzieller Wert und das enorme Überwachungspotential der modernen Informationstechnik bedrohen darüber hinaus die Privatsphäre der Bürger in fundamentaler Weise. Die – oft heimliche – Sammlung, Verknüpfung und Deanonymisierung personenbezogener Daten zu wirtschaftlichen Zwecken haben inzwischen Orwells Bedrohungsszenarien von der staatlichen Überwachung auf private Datensammlungen verlagert, die aber auch von Sicherheitsbehörden genutzt werden können.

Erhebliche praktische Bedeutung haben zudem klassische Delikte wie der Betrug, bei denen das Internet als Tatwerkzeug dient. Anonymität und transnationale Deliktsbegehung im globalen Cyberspace erleichtern die Tatbegehung und erschweren die Strafverfolgung. Die Straftäter schützen sich zusätzlich durch Anonymisierungsdienste gegen eine Rückverfolgung und setzen auf ihren Rechnern Verschlüsselungen ein, die als solche nicht mehr gebrochen werden können. Die Ermittlungen sind weiter erschwert, wenn – etwa beim Cloud-Computing – kritische Daten auf Rechner in aller Welt verteilt werden, die Behörden jedoch nur auf ihrem Territorium ermitteln können und fremde Souveränitätsrechte auf ausländischen Servern respektieren müssen. Die Leistungsfähigkeit des Internets führt gleichzeitig allerdings auch zu neuen Überwachungs- und Kontrollmöglichkeiten, welche die Prävention und Repression von Straftaten verbessern können.



DIE INFORMATIONSTECHNISCHE INFRASTRUKTUR DER MODERNEN GESELLSCHAFT KANN DAHER IN BESONDEREM MASSE VON WELTWEIT AGIERENDEN TÄTERN ÜBER DAS INTERNET ANGEGRIFFEN WERDEN.

IM FOKUS: NEUE ANGRIFFE AUF DIE INTEGRITÄT VON COMPUTERSYSTEMEN

Die verschiedenen Deliktsformen der Internetkriminalität treten nicht nur isoliert voneinander auf, sondern stehen aufgrund arbeitsteilig organisierter Täterstrukturen oft in einem Zusammenhang. So arbeiten „Spezialisten" an der Entdeckung von Sicherheitslücken in Computersystemen (sog. Exploits), während andere Tätergruppen auf diese Lücken angepasste Schadsoftware entwickeln. Entdeckt der potentielle Täter eine solche Schwachstelle etwa in einer Browsersoftware, so kann er eine Webseite präparieren, die jedes sie abrufende Computersystem infiltriert. Diese sog. Drive-by-Exploits sind mittlerweile neben E-Mails mit angehängten Schaddateien die wichtigste Methode zur Verbreitung von Schadsoftware. Mittels dieser können die Täter auf alle von einem Nutzer gespeicherten Dateien zugreifen und so auch seine „digitale Identität" weitestgehend übernehmen.

Besonders interessant sind für die Angreifer dabei Kreditkarteninformationen sowie Zugangsdaten, etwa zu Bankkonten, Online-Zahlungsdiensten oder Online-„Auktionsplattformen" wie eBay. Diese Daten werden über versteckt betriebene Online-Foren des Untergrundmarktes bündelweise verkauft. Anschließend wird dann im Wege klassischer Delikte wie dem Computerbetrug die eigentliche Wertschöpfung betrieben, etwa durch Plünderung von Konten oder durch Nutzung der erlangten Identität für eine betrügerische Handlung. Ein anderer Weg zur Erlangung fremder Nutzerdaten sind sog. Phishing-Mails, bei denen das Opfer durch Vorgabe einer falschen Identität dazu motiviert wird, persönliche Daten über eine vermeintlich vertrauenswürdige Webseite zu übermitteln. Diese Methode ist inzwischen allerdings – auch wegen umfangreicher Aufklärungskampagnen – weniger erfolgreich als die zuvor beschriebene.

Neben diesen breit gestreuten Angriffen, die zumeist Privatpersonen betreffen, nehmen auch gezielte Angriffe auf Unternehmen und staatliche Einrichtungen stetig zu. So waren nach Presseberichten 2007 im Vorfeld einer Wirtschaftsreise der deutschen Bundeskanzlerin in ein bestimmtes Land die Rechner des Kanzleramts und zahlreicher Ministerien von einer Schadsoftware befallen, die große Datenmengen abfing und an Server in dem zu besuchenden Land weiterleitete. Heute erfolgen täglich etwa vier gezielte Angriffe auf die Computer der deutschen Bundesregierung. Noch gravierendere Cyberangriffe sind im Rahmen kriegerischer Auseinandersetzungen oder aus terroristischen Motiven möglich, etwa durch gezieltes Einwirken auf sicherheitsrelevante Infrastruktureinrichtungen wie Krankenhäuser oder Kraftwerke. Ein groß angelegter Angriff störte beispielsweise in Estland im Jahr 2007 die Internetnutzung für mehrere Wochen schwer, so dass Geldautomaten und Kommunikationsnetze der Polizei nur noch sehr eingeschränkt funktionierten. Als Angriffsmittel dienten sog. DDoS-Angriffe, bei denen unzählige einzelne Computersysteme (sog. bots) massenhaft gleichzeitige (oft sinnlose) Anfragen an ein einzelnes Zielsystem stellen, so dass dieses unter der Last des Datenaufkommens zusammenbricht.

Bots sind Computersysteme, die – beispielsweise mit der beschriebenen Methode des Drive-by-Exploits – durch Schadsoftware infiziert werden und sich über diese Schnittstelle durch den Angreifer entsprechend fernsteuern lassen, meist ohne dass der Besitzer des Computers dies überhaupt bemerkt. In einzelnen Fällen stellten die Ermittler riesige „Bot-Armeen" fest, bei denen die Täter mehrere Millionen infizierte fremde Rechner unter ihrer Kontrolle hatten. Entsprechende Botnet-Kapazitäten lassen sich über die Kommunikationsplattformen des Untergrundmarktes innerhalb weniger Minuten je nach Bedarf anmieten und dann gegen bestimmte Rechner richten. Dieses Angriffsmittel wird inzwischen zunehmend genutzt, um Unternehmen zu kritischen Zeitpunkten mit dem Ausfall ihrer Netzinfrastruktur zu bedrohen und zu erpressen.

TECHNISCHER UND RECHTLICHER SCHUTZ

Die Analyse der einschlägigen Bedrohungslagen und Fälle zeigt, dass die Sicherheit moderner Computersysteme primär durch technische, organisatorische und personelle Schutzmaßnahmen gewährleistet werden muss. Erforderlich sind daher zunächst sichere Informations- und Kommunikationssysteme sowie die Aufklärung ihrer Nutzer über die Risiken von digitalen Daten- und Kommunikationsgeräten. In dem notwendigen kriminalpolitischen Gesamtkonzept haben jedoch auch rechtliche Maßnahmen eine hohe Bedeutung, weil sie die Grenzen des Erlaubten verbindlich klären sowie Verbote und Gebote mit staatlichen Sanktionen und Zwangsmitteln durchsetzen können. Strafrecht und Polizeirecht sind darüber hinaus wichtig, weil nur sie die erforderlichen Zwangsmittel für die Verfolgung und Prävention der Delikte und insbesondere die Rückverfolgung von Angreifern im Internet bereitstellen und dabei auch Amts- und Rechtshilfe für Auslandsermittlungen ermöglichen. Bei eingriffsintensiven Sicherheitsmaßnahmen kann auch nur das Recht garantieren, dass die Freiheit der Bürger und ihre Persönlichkeitsrechte nicht unverhältnismäßig eingeschränkt werden. Die Abwägung von Sicherheits- und Freiheitsinteressen sowie die Entwicklung der entsprechenden Ausgleichsmechanismen ist daher eine zentrale Aufgabe des neu zu konzipierenden Informationssicherheitsrechts.

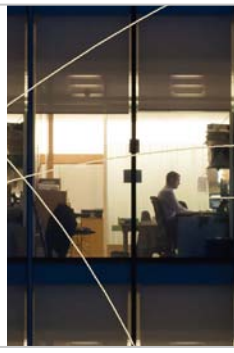
Die rechtlichen Maßnahmen zur Verhinderung von Internetkriminalität erfordern ein umfassendes Konzept unter Einbeziehung verschiedener Rechtsregime und Regelungsmodelle. Dazu gehören das Strafrecht, das Polizeirecht, das Gefahrenvorsorgerecht, das Recht der Nachrichtendienste, das Telekommunikationsrecht u.a.m. Die Wirksamkeit rechtlicher Regelungen hängt im globalen Cyberspace darüber hinaus auch stark von dem bestehenden internationalen Kooperationsrecht und geeigneten internationalen Institutionen ab. Strafrechtliche Normen können weiter durch eine Selbst- und Koregulierung der Wirtschaft unter Einbeziehung von public-private partnerships ergänzt werden. In Einzelfällen wie beim Urheberrechtsschutz stellt sich die – vor allem auch theoretisch interessante – Frage, inwieweit z.B. das Zivil- oder das Zollrecht funktionale Äquivalente für bestimmte Maßnahmen der Strafverfolgung bieten können. Eine Verknüpfung der unterschiedlichen Rechtsgebiete und die Verbindung ihrer Institutionen in einer integrierten Sicherheitsarchitektur mit übergreifenden Abwehrzentren versprechen dabei eine sehr viel effektivere Kriminalpolitik. Eine solche Flexibilisierung der klassischen Teilrechtsgebiete muss allerdings die – oft gebietsspezifischen – rechtsstaatlichen Garantien dieser Teildisziplinen besonders berücksichtigen.

ZIELE UND METHODEN DER MAX-PLANCK-FORSCHUNG

Der Forschungsschwerpunkt „Cybercrime“ am Freiburger Max-Planck-Institut für ausländisches und internationales Strafrecht zielt auf eine umfassende Analyse der einschlägigen Delikte und der entsprechenden – vor allem strafrechtlichen – Normen. Auf dieser Grundlage sollen die notwendigen Teile des Sicherheitsrechts für den globalen Cyberspace neu bestimmt werden. Dieses Recht muss den einzelnen Bürger und die Gesellschaft gegen kriminelle Bedrohungen schützen, gleichzeitig aber auch die Freiheitsrechte der Bürger gegenüber dem Staat und der Wirtschaft bewahren, die zumindest im Internet den Schlüssel für eine Orwellsche Totalüberwachung bereits in den Händen halten. Bei der Klärung der Grundlagenfragen und der Entwicklung neuer Lösungen werden empirisch-kriminologische, rechtsvergleichende und rechtsdogmatische Methoden kombiniert.

Voraussetzung und Grundlage der Entwicklung des neuen Informationsstrafrechts ist daher zunächst eine empirisch-kriminologische Analyse, die technische Grundlagen sowie einschlägige Bedrohungen untersucht und Voraussetzung einer jeden seriösen Kriminalpolitik ist. Der hierfür notwendige interdisziplinäre Ansatz wird durch die Struktur des Freiburger Max-Planck-Instituts erleichtert, das über eine strafrechtliche und eine kriminologische Abteilung verfügt. Hinzu kommt die interdisziplinäre Zusammenarbeit mit den Informatikern vor allem von der Universität Freiburg. Zentral ist weiter die rechtsvergleichende Untersuchung, die neben den deutschen Regelungen auch die unterschiedlichen ausländischen und internationalen Lösungsansätze einbezieht. Der Vergleich mit ausländischen Lösungen, der ein Markenzeichen aller juristischen Max-Planck-Institute ist, relativiert den eigenen Standpunkt, vermittelt zahlreiche neue Lösungsansätze und erleichtert die notwendigen Kooperationen in der immer enger zusammenwachsenden globalen Welt. Mit einer der weltweit größten Bibliotheken in den Bereichen der Strafrechtsvergleichung und der Kriminologie, spezialisierten Mitarbeite-

DIE SAMMLUNG, VERKNÜPFUNG UND DEANONYMISIERUNG PERSONENBEZOGENER DATEN ZU WIRTSCHAFTLICHEN ZWECKEN HABEN INZWISCHEN ORWELLS BEDROHUNGSSZENARIEN VON DER STAATLICHEN ÜBERWACHUNG AUF PRIVATE DATENSAMMLUNGEN VERLAGERT, DIE ABER AUCH VON SICHERHEITSBEHÖRDEN GENUTZT WERDEN KÖNNEN.



rinnen und Mitarbeitern sowie einem großen Netzwerk von ausländischen Kooperationspartnern und -partnerinnen ist das Freiburger Institut hierfür prädestiniert. Die Kombination der verschiedenen empirischen, rechtsvergleichenden und rechtsdogmatischen Methoden der Grundlagenforschung bietet einen fruchtbaren Nährboden für eigene Analysen, Ideen und Lösungen.

ERGEBNISSE DER GRUNDLAGENFORSCHUNG ALS BASIS FÜR PRAKTISCHE REFORMEN

Die Ergebnisse der Grundlagenforschung zu den Besonderheiten des Informationsrechts kommen auch der Lösung von Reformfragen zugute. Von zentraler Bedeutung ist hierbei die immaterielle Natur von Daten. Diese weisen wesentliche Spezifika gegenüber den klassischen körperlichen Rechtsobjekten auf, die im 19. und 20. Jahrhundert dominierten und die Rechtsregeln prägten. Aufgrund dieser Besonderheiten können informationsrechtliche Fragestellungen nicht einfach dadurch gelöst werden, dass die für körperliche Gegenstände entwickelten Normen unreflektiert auf Daten und Informationen angewandt werden. Der Mathematiker Norbert Wiener (1894-1964) brachte diese Besonderheiten mit dem Satz auf den Punkt, "Information is information, not matter or energy. No materialism which does not admit this can survive at the present day." Es ist bemerkenswert, dass diese ontologische Definition des Begründers der modernen Informationstheorie und der Kybernetik „Information" auf eine Stufe mit „Materie" und „Energie", den Grundkategorien des modernen wissenschaftlichen Weltverständnisses, stellt. Die Erkenntnis der Kybernetik, Information sei weder Materie noch Energie, sondern eine dritte „Grundgröße", ist für die Rechtswissenschaften ein wichtiger Hinweis, die noch immer verbreitete Lösung informationsrechtlicher Fragen mit den für körperliche Sachen entwickelten Rechtsregeln in jedem Einzelfall kritisch zu hinterfragen und – wie im klassischen Immaterialgüterrecht seit Langem bekannt – zwischen (körperlichem) Datenträger, (unkörperlichen) Daten und der in ihnen enthaltenen Information zu unterscheiden. Diese und weitere Aspekte müssen daher in eine Theorie des Informationsrechts und des Informationsstrafrechts integriert werden.

IN EINZELNEN FÄLLEN STELLTEN DIE ERMITTLER RIESIGE „BOT-ARMEEN" FEST, BEI DENEN DIE TÄTER MEHRERE MILLIONEN INFIZIERTE FREMDE RECHNER UNTER IHRER KONTROLLE HATTEN.

Herausragende Bedeutung für die dogmatische Konzeption und die praktische Ausgestaltung des damit entstehenden eigenständigen Informationsrechts haben auch der globale Charakter des Cyberspace, die damit gegebenen einfachen Möglichkeiten der weltweiten Datenübermittlung und die hieraus resultierende transnationale Kriminalität. Staatsgrenzen spielen daher bei Internetstraftaten eine sehr viel geringere Rolle als im Bereich der klassischen Kriminalität, da territoriale Grenzen und entsprechende Kontrollen im weltweiten Datennetz nur schwer durchsetzbar sind. Straftäter können somit leicht in ein Land mit einer günstigen Gesetzgebung oder einem Vollzugsdefizit ausweichen. Rechtliche Lösungen funktionieren deswegen in vielen Bereichen nur, wenn ein internationaler Konsens besteht.

Hinzu kommen die häufige Anonymität der Angreifer und die daraus entstehenden technischen Probleme bei der Identifizierung der Täter. Die – vom Freiburger Institut aktiv mitgestalteten – aktuellen Diskussionen um die Online-Durchsuchung, den sog. „Staatstrojaner" zur Quelldatenkommunikationsüberwachung oder die Vorratsdatenspeicherung zeigen, dass dies zu schwierigen Abwägungen zwischen den Sicherheitsinteressen der Gesellschaft und dem Freiheits- und Persönlichkeitsrechtsschutz der Bürger führt. Anonymität und Distanz im Internet verursachen auch unterschiedliche Konzepte von sozialem Vertrauen in körperlichen und in virtuellen Welten. Diese sind etwa bei der Beurteilung von verdeckten Ermittlungen der Sicherheitsbehörden in sozialen Netzwerken relevant, bei denen das derzeit beginnende data mining der Sicherheitsbehörden neue Fundgruben von ermittlungsrelevantem Wissen schafft, deren Nutzung geregelt sein muss. Der rasche technische Wandel ist ein weiteres Spezifikum der virtuellen Welt, das die rechtliche Regulierung zusätzlich erschwert. Er zwingt zu einer permanenten Anpassung des Rechts, das den laufenden Innovationsprozess durch funktionale und technikneutrale Regelungen so weit wie möglich vorwegnehmen muss.

ENTWICKLUNG ANWENDUNGSORIENTIERTER LÖSUNGEN

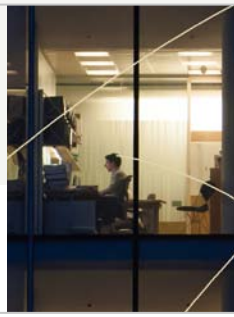
Die Charakteristika von Information bestimmen in vielerlei Hinsicht auch die Inhalte des zukünftigen Informationsstrafrechts. Sie bestätigen z.B. die Erkenntnis, dass die unberechtigte Erlangung von Information nicht mit dem klassischen Diebstahlstatbestand erfasst werden kann, da dieses – für körperliche Gegenstände entwickelte – Delikt eine Enteignung beim Opfer verlangt, die bei der Kopie von Information nicht gegeben ist. Im Bereich des materiellen Strafrechts zeigen sich die spezifischen Schutzbedürfnisse auch an dem

neu geschaffenen Straftatbestand des unbefugten Sich-Verschaffens von zugriffsgesicherten Daten, der u.a. die Integrität von Computersystemen gegen Hacking schützt.

Im Strafprozessrecht erfolgen Durchsuchungen, Beschlagnahmen und Herausgabeverlangen von Datenbeständen dagegen heute noch immer nach den klassischen Vorschriften für Sachen, die viele Besonderheiten von Daten nicht berücksichtigen. Anders als bei der Herausgabe von körperlichen Gegenständen stellt sich beim staatlichen Zwangszugriff auf Daten z.B. die Frage nach den Möglichkeiten einer Datenkopie (statt der Wegnahme der körperlichen Datenträger), nach der eventuellen Verpflichtung von Zeugen zum Ausdruck verschlüsselter Daten im Klartext oder – noch viel eingriffsintensiver – zur Bekanntgabe oder Aushändigung von Passwörtern und Zugriffsschlüsseln, die den Ermittlungsbehörden einen vollständigen Zugriff auf das Datensystem gibt. Werden E-Mails beim Mail-Provider beschlagnahmt, so ist zu entscheiden, ob in einem solchen Fall die Daten bereits auf der Empfängerseite angekommen sind und mit den großzügigeren Beschlagnahmevorschriften sichergestellt werden können oder ob hier mit den wesentlich strengeren Vorschriften über die Telekommunikationsüberwachung noch in einen laufenden Übertragungsprozess eingegriffen wird.

Fragwürdig und nach den Ergebnissen des Freiburger Instituts verfassungswidrig ist die gegenwärtige Praxis, bei verschlüsselter Datenübertragung unter Berufung auf die Vorschriften zur Überwachung der Telekommunikation heimlich in miteinander kommunizierende Rechner einzudringen und die Daten dort an der noch unverschlüsselten Quelle abzugreifen. Eine solche „Quellentelekommunikationsüberwachung“ stellt in der Sache eine „kleine“ Online-Durchsuchung dar, die in der Strafprozessordnung zur Strafverfolgung – anders als im BKA-Gesetz zur Gefahrenabwehr – nicht vorgesehen ist und für die das Bundesverfassungsgericht spezielle rechtliche und technische Schutzmaßnahmen gefordert hat. Diese besonderen Vorschriften fehlen jedoch in der gegenwärtigen Bestimmung über die Telekommunikationsüberwachung. Für die damit notwendige Neuregelung ist beispielsweise auch zu klären, ob der Datenaustausch mit dem Cloudanbieter eine „Telekommunikation“ darstellt, die von der Justiz noch mit den Vorschriften der Telekommunikationsüberwachung abgegriffen werden kann, oder ob es bei einer funktionalen Betrachtung nur um die Kommunikation mit den eigenen Daten geht, die allein mit einer – für die Strafverfolgung derzeit abgelehnten – „großen“ Online-Durchsuchung möglich wäre. Diese Problematik wird – ebenso wie zahlreiche andere in einer aktuellen Institutsarbeit aufgezeigte neue Fragestellungen – in der bisherigen Rechtsprechung und Literatur noch nicht einmal im Ansatz diskutiert.

DIESES RECHT MUSS DEN EINZELNEN BÜRGER UND DIE GESELLSCHAFT GEGEN KRIMINELLE BEDROHUNGEN SCHÜTZEN, GLEICHZEITIG ABER AUCH DIE FREIHEITSRECHTE DER BÜRGER GEGENÜBER DEM STAAT UND DER WIRTSCHAFT BEWAHREN, DIE ZUMINDEST IM INTERNET DEN SCHLÜSSEL FÜR EINE TOTALÜBERWACHUNG BEREITS IN DEN HÄNDEN HALTEN.

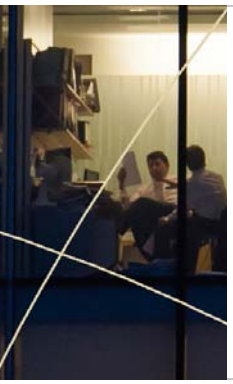


Noch kaum geklärt sind auch die Fragen, die aus der globalen Natur des Cyberspace resultieren. Hier ist weitgehend ungeklärt, inwieweit die Ermittlungsbehörden im weltumspannenden Internet auf ausländischen Servern agieren können. Nach herrschender Meinung verstößt dies zumindest bei nicht-öffentlichen Informationsangeboten gegen die Souveränität des Staates, auf dessen Territorium der Server steht. Wenn diese Regelungen ernst genommen werden und keine neuen Lösungsansätze bei der Amts- und Rechtshilfe oder der Schaffung neuer Strafverfolgungsinstitutionen für den Cyberspace gefunden werden, dann dürften sich bald erhebliche Schwierigkeiten ergeben. Dies gilt wiederum besonders beim Cloud-Computing, bei dem oft nicht einmal den Beteiligten bekannt ist, auf welchem Territorium die in der globalen Wolke gesuchten Daten sich gerade befinden.

Die gescheiterten Versuche von Internetsperren gegen Kinderpornografie haben – auch in Gutachten des Freiburger Instituts – deutlich gemacht, dass die alten Schutzkonzepte einer Abschottung der Nationalstaaten gegenüber fremden Territorien im Internet schon lange nicht mehr möglich sind. Die klassischen Konzepte der Souveränität, der Territorialität und der Amts- und Rechtshilfe werden daher fundamental herausgefordert, wenn riesige Datenmengen des Internets in Millisekunden um die Welt bewegt werden. Auch insoweit sind die traditionellen Regelungen über die Grenzkontrolle körperlicher Gegenstände zum Scheitern verurteilt und neue Lösungskonzepte gefragt.

UMSETZUNG DER ERGEBNISSE IN DIE RECHTSPOLITIK

Die Grundlagenforschung des Freiburger Instituts fließt in vielfältiger Weise in die Lösung von praktischen Problemstellungen ein. Beispiele für diesen Transfer der Forschungsergebnisse in die aktuelle Rechtspolitik waren in der Vergangenheit die Anhörungen des Bundesverfassungsgerichts zur Online-Durchsuchung, die Beratungen verschiedener Bundestagsausschüsse zu Internetsperren und zu den neuen Vorfelddelikten gegen terroristische Propaganda, die internationale Abstimmung des Europarats über die Verhinderung von Cyberterrorismus oder die neuen Ansätze der Vereinten Nationen zur Entwicklung von weltweiten Gesetzesstandards im Bereich des Cybercrime. Die im Freiburger Institut erarbeiteten jüngsten Vorschläge für eine Gesamtreform des deutschen Informationsstrafrechts werden nunmehr auch den Ausgangspunkt für die Beratungen des nächsten Deutschen Juristentages im September 2012 in München bilden.



DIE ERKENNTNIS DER KYBERNETIK, INFORMATION SEI WEDER MATERIE NOCH ENERGIE, SONDERN EINE DRITTE „GRUNDGRÖSSE", IST FÜR DIE RECHTSWISSENSCHAFTEN EIN WICHTIGER HINWEIS, DIE NOCH IMMER VERBREITETE LÖSUNG INFORMATIONSRECHTLICHER FRAGEN MIT DEN FÜR KÖRPERLICHE SACHEN ENTWICKELTEN RECHTSREGELN IN JEDEM EINZELFALL KRITISCH ZU HINTERFRAGEN.

Die grundlagenbasierten und theoriegeleiteten Aktivitäten machen deutlich, wie hilfreich in den Rechtswissenschaften Ergebnisse der Grundlagenforschung für praktische Fragestellungen sein können und wie viele Anregungen die Grundlagenforschung erhält, wenn sie sich auf praktische Fragen einlässt. Die Entwicklung des Informationsrechts im Cyberspace belegt nicht nur den Physiker Max Planck mit seinem Zitat „Dem Anwenden muss das Erkennen vorausgehen". Sie bestätigt auch den dem Philosophen und Rechtswissenschaftler Immanuel Kant zugeschriebenen Satz: „Es gibt nichts Praktischeres als eine gute Theorie."

Literatur:

Ulrich Sieber, Straftaten und Strafverfolgung im Internet – Welche Maßnahmen empfehlen sich im Hinblick auf die neuen Herausforderungen der globalen Informationsgesellschaft?, Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 69. Deutschen Juristentages, München 2012, S. C 1 – 148.

ders., Mastering Complexity in the Global Cyberspace, in: Mireille Delmas-Marty/ Mark Pieth/ Ulrich Sieber (Hrsg.), Les chemins de l'harmonisation pénale, Paris 2008, S. 127 – 202.

ders., Rechtliche Ordnung in einer globalen Welt, Rechtstheorie 41 (2010), S. 151 – 198 (engl. Übersetzung: Legal Order in a Global World, in: A. von Bogdandy/ R. Wolfrum, ed., Max Planck Yearbook of United Nations Law Vol. 14, 2010, S. 1 – 49).

PROF. DR. DR. H.C. MULT. ULRICH SIEBER,
MAX PLANCK INSTITUTE FOR FOREIGN AND INTERNATIONAL CRIMINAL LAW, FREIBURG IM BREISGAU

Cybercrime and criminal law in the global information society

In accordance with its research programme, the department of criminal law at the Max Planck Institute for Foreign and International Criminal Law in Freiburg analyses the changes taking place in crime and criminal law in the global information and risk society. Areas of emphasis include terrorism, international criminal law, organised crime, economic crime and computer crime. The project presented here, "Cybercrime and Criminal Law in the Global Information Society," examines by means of empirical, comparative legal and doctrinal methods the evolution of information technology, crime and law in the modern information and network society. The goal is the analysis of relevant offenses and their – national and international – regulation as well as the development of new criminal policy concepts with which to respond to new challenges. The inclusion of theoretical principles of information criminal law contributes to the development of application-oriented solutions that take into account the intangible nature of data, the global character of cyberspace and the anonymity of the Internet.

VULNERABILITY OF THE INFORMATION SOCIETY

Crime committed on the Internet poses an existential risk to the modern information society, the main threats being attacks on the integrity of computer systems, especially hacking, manipulation and destruction of data, as well as the spreading of malicious software (malware) and the unauthorised obtaining of access codes. These crimes jeopardise the very foundations of the economy, governmental agencies and the private sector, which depend on secure processing of data and data communication. The reliability of information- and communication systems is particularly at risk, as they are often inadequately protected due to design weaknesses in the software and user carelessness. As a result, the IT infrastructure of modern society is vulnerable to attack via the Internet by globally operating perpetrators. This is true for computers used in businesses, for information technology in the public sector and for the PC of each and every individual Internet user as well as for the computer systems of banks, manufacturing companies, governmental agencies and the military and those of nuclear power plants, hospitals and aircraft.

Similarly, illegal online content poses major risks: in cyberspace, large amounts of data can be distributed quickly to all four corners of the world without being subjected to effective state control mechanisms. Access to child pornography is also considerably facilitated by communication opportunities and the anonymity that the Internet offers. However, the difficulties in controlling data also manifest themselves in large-scale copyright violations, cross-border gambling, illegal marketing of products and terrorist or extremist propaganda in the Internet.

Moreover, the large volume of personal data stored by government and commercial enterprises, their considerable commercial value and the enormous potential for surveillance harboured by modern information technology constitute fundamental threats to the privacy of individuals. The – often secret – collection, collation and deanonymisation of personal data for commercial purposes have now shifted *Orwell's* threat scenarios of state surveillance to the private sector's databases, which may also, however, be used by security authorities.

THE IT INFRASTRUCTURE OF MODERN SOCIETY IS VULNERABLE TO ATTACK VIA THE INTERNET BY GLOBALLY OPERATING PERPETRATORS

The Internet also serves as a convenient tool for *traditional crimes*, such as fraud. Anonymity and the transnational dimension of global cyberspace often facilitate the commission of offences and render prosecution difficult. In addition, perpetrators protect themselves against tracing by using anonymisation services and employing encryption on their computers that cannot be deciphered. Criminal investigations become even more difficult when – as with cloud computing – critical information is stored on computers located all over the world but authorities may only investigate within their own territory and must not violate foreign sovereignty over servers in other countries. At the same time, the capabilities of the Internet open up new possibilities for surveillance and control, which can be used to improve crime prevention and law enforcement.

FOCUS: NEW ATTACKS ON THE INTEGRITY OF COMPUTER SYSTEMS

While the various types of Internet crime can be committed as isolated offences, they are – due to the nature of the Internet – often committed in clusters by separate groups of offenders, each of which has expertise in one or more aspects of information technology. For example, one group of "specialists" may work on discovering vulnerabilities in computer systems, while other groups of perpetrators develop malicious software tailored to these vulnerabilities (so-called

exploits). If the potential perpetrator discovers a weakness, say, in browser software, he or she can prepare a website which infiltrates each computer system that opens the site. In the meantime, with the exception of e-mail with malicious attachments, these so-called *drive-by exploits* have become the most common method of spreading malware. They can be used by perpetrators to access a user's stored files and, with the help of the information garnered, to assume his or her "digital identity."

THE – OFTEN SECRET – COLLECTION, COLLATION AND DEANONYMISATION OF PERSONAL DATA FOR COMMERCIAL PURPOSES HAVE NOW SHIFTED ORWELL'S THREAT SCENARIOS OF STATE SURVEILLANCE TO THE PRIVATE SECTOR'S DATABASES, WHICH MAY ALSO, HOWEVER, BE USED BY SECURITY AUTHORITIES.

Attackers are particularly interested in credit card details and access codes to, for example, bank accounts, online payment services and online auction sites such as eBay. This kind of information is sold in bundles via covert online forums on the black market. The actual profit is made subsequently, by means of such traditional crimes as computer fraud, in which, for instance, bank accounts are plundered or the assumed identity used for fraudulent actions. Another way to gain access to people's user data is to send so-called phishing e-mails, which, with the help of a false identity, try to induce victims to reveal personal information via an apparently trustworthy website. The latter method, however, is now less successful than the former, due in part to extensive information campaigns.

In addition to these widely spread attacks, which mostly affect private individuals, attacks specifically targeting companies and governmental institutions are steadily increasing. According to press reports, prior to an official visit by the German chancellor to a certain country in 2007, the computers in numerous governmental departments were infected with malicious software which intercepted large amounts of data and forwarded them to servers in the country to be visited. Today, some four attacks targeting the computers of the German government take place every day. Cyber attacks that are even more serious are possible in the context of armed conflicts or terrorist-motivated aggression. This kind of attack could target infrastructure relevant for safety, such as hospitals or power plants. An example of such an attack is the one that disrupted Internet access in Estonia for several weeks in 2007 and severely hampered the operation of ATMs and police communication networks. In this case, *distributed denial-of-service attacks* (DDoS) were used. This method of attack makes use of countless autonomous computers (so-called *bots*) to saturate a single target system with simultaneous (and often pointless) requests in order to cause the target system to crash because of the data traffic generated.

Bots are computers that have been infected with malicious software (e.g. by means of a drive-by exploit as described above) and can be controlled remotely by the attacker via this interface, usually without the owner of the computer even noticing. In some cases, investigators have identified vast "bot armies" where the perpetrators controlled the infected computers of several million users. Botnet capacities tailored to the needs of the client can be rented via black-market communication platforms in a matter of minutes and ordered to target specific computers. In the meantime, this method of attack is being used more and more often to threaten companies – for the purpose of extortion – with network infrastructure failure at critical points in time.

TECHNICAL AND LEGAL PROTECTION

The analysis of relevant threats shows that protective measures in three primary areas, namely, *technology, organisation and personnel*, are necessary to ensure the security of modern computer systems. Thus, secure information- and communication systems are a must, and users have to be educated about the risks inherent in digital data- and communication devices. Legal measures are also very important in a necessarily comprehensive approach to criminal policy, however, as they establish binding limits on the permissible and enable the enforcement of prohibitions and requirements through governmental sanctions and coercive measures. Criminal law and police law are particularly important, as only they are authorized to employ the necessary coercive measures when prosecuting and preventing crime and, perhaps even more importantly, when tracing attackers on the Internet; furthermore, these areas of law have access to administrative and legal cooperation in international investigations. And as for intrusive security measures, only the law can guarantee that the freedom of individuals and their personality rights are not disproportionately restricted. Striking a balance between the interests of security and those of liberty and developing the appropriate balancing mechanisms are therefore key challenges for the newly emerging information security law.

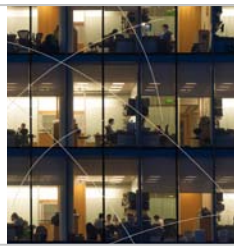
Legal measures to prevent Internet crime need to be embedded in a comprehensive concept which incorporates a *variety of legal regimes and regulatory models*. These include, criminal law, police law and other danger prevention law, intelligence law and telecommunications law. Moreover, the enforceability of legal regulations in global cyberspace depends, to a large extent, on existing international cooperation law and suitable international institutions. Criminal law norms may also be supplemented by the self- and co-regulation of the private sector with the help of *public-private partnerships*. Some cases, the protection of copyright, for instance, also raise the question of whether civil or customs law could offer functional equivalents in place of selected law enforcement measures. Combining different legal areas and linking their institutions in an integrated security architecture with comprehensive defence centres could very well render a significantly more effective criminal policy. Above all, however, this kind of flexibility combining the traditional branches of law must take into consideration the rule-of-law guarantees that are often linked to one or the other of those branches.

OBJECTIVES AND METHODS OF MAX PLANCK RESEARCH

The goal of research focusing on cybercrime at the Max Planck Institute for Foreign and International Criminal Law is to produce a comprehensive analysis of relevant offences and the corresponding – primarily criminal law – norms. On this basis, the necessary components of security law for the global cyberspace will be redefined. This new law must protect individuals and society against criminal threats, but at the same time safeguard individuals' civil liberties against intervention from both the state and the private sector, which, taken together already have the means for an *Orwellian* kind of mass surveillance – at least on the Internet. Methods of empirical criminology, comparative law and legal doctrine are combined to solve fundamental issues and develop new solutions.

The basis for developing a new information criminal law is, first and foremost, an *empirical criminological analysis* that evaluates the technical bases and associated threats and is a prerequisite for any serious criminal policy. The interdisciplinary approach necessary for this analysis is facilitated by the structure of the Freiburg-based Max Planck Institute, which hosts a department each for criminal law and criminology. Interdisciplinary cooperation with computer scientists at (mainly) the University of Freiburg is another advantage. Another key element is the *comparative legal study* that, in addition to German strategies, examines the various foreign and international approaches. The comparison with foreign solutions, which is characteristic of all the law-related Max Planck Institutes, serves to put one's own position into perspective, offers many new solutions and facilitates the collaboration that is necessary in an increasingly interconnected global world. Thanks to one of the largest libraries worldwide on comparative criminal law and criminology, specialised staff and a large network of foreign partners, the Institute in Freiburg is predestined for this type of research. The combination of the basic research methods of empirical criminology, comparative law and legal doctrine provides a fertile ground for developing creative analyses, ideas and solutions.

IN SOME CASES, INVESTIGATORS HAVE IDENTIFIED VAST "BOT ARMIES" WHERE THE PERPETRATORS CONTROLLED THE INFECTED COMPUTERS OF SEVERAL MILLION USERS.



RESULTS OF BASIC RESEARCH AS THE BASIS FOR PRACTICAL REFORMS

The results of basic research on the particularities of information law can also be used to resolve reform-related issues. The *intangible nature of data* is significant in this context. Specific characteristics set data apart from the classic, tangible legal objects which dominated the 19th and 20th centuries and informed legal regulation. Because of these particularities, problems associated with information law cannot be solved simply by applying norms developed with physical objects in mind to data and information. The mathematician *Norbert Wiener (1894–1964)* summed up these peculiarities in the following statement: "Information is information, not matter or energy. No materialism which does not admit this can survive at the present day." It is remarkable that this ontological definition from the founder of modern information theory and cybernetics places "information" on a level with "matter" and "energy," the basic categories used in the modern scientific understanding of the world. The insight stemming from cybernetics that information is neither matter nor energy, but a third "basic variable" is an important reminder for legal science, first, to challenge the way in which information law-related problems are still largely solved, namely, by applying the rules developed for physical objects, and, second, to distinguish between (tangible) data storage media, (intangible) data and the information that they contain – a distinction that is

already well-established in traditional intellectual property law. In sum, these and additional considerations must be integrated into a theory of information law and information criminal law.

The global character of cyberspace, the simple means of worldwide data transmission that it offers and the resulting transnational crime are all of utmost importance for the doctrinal conception and the practical design of the emerging, free-standing information law. National borders are far less important in the context of Internet crime than in the context of conventional crime, as territorial borders and the controls that go with them are very hard to enforce in the global data network. Perpetrators can easily relocate to a country with an advantageous set of laws or lax enforcement. Thus, in many fields, legal solutions function only if an international consensus has been reached.

THIS NEW LAW MUST PROTECT INDIVIDUALS AND SOCIETY AGAINST CRIMINAL THREATS, BUT AT THE SAME TIME SAFEGUARD INDIVIDUALS' CIVIL LIBERTIES AGAINST INTERVENTION FROM BOTH THE STATE AND THE PRIVATE SECTOR, WHICH, TAKEN TOGETHER ALREADY HAVE THE MEANS FOR A KIND OF MASS SURVEILLANCE – AT LEAST ON THE INTERNET.

Add to this the frequent *anonymity of attackers* and the technical problems that arise when attempts are made to identify the perpetrators. The current debates on online searches, on the so-called "government Trojan" for the surveillance of telecommunications data at the source as well as on data retention – all actively shaped by the Institute in Freiburg – show that these practices lead to difficult trade-offs between the security interests of society and the protection of individual civil liberties and personality rights. The anonymity and distance on the Internet also give rise to different concepts of *social trust* in the physical and virtual worlds. These differences are relevant, for instance, when evaluating covert intelligence operations by governmental security agencies in social networks. The emerging method of *data mining* employed by security agencies generates new caches of information relevant for investigations, the use of which must be regulated. *Rapid changes in technology,* also characteristic of the virtual world, make legal regulation even more difficult. Due to the rapid pace of change, continuous updating of the law is necessary in order for it even to begin to anticipate, by means of functional and technologically-neutral regulations, the ongoing process of innovation.

DEVELOPING APPLICATION-ORIENTED SOLUTIONS

In many respects, the characteristics of information also determine the content of the future criminal law of information. They confirm the realisation that the unauthorised interception of information cannot be covered by the traditional theft offence definition, since this offence, which was defined with physical objects in mind, requires a dispossession of the victim that does not occur when information is copied. In the area of substantive criminal law, the need for specific protective measures can be seen in the newly created offence of the unauthorised procuring of secured data, which serves among other things to protect the integrity of computer systems against hacking.

As far as the law of criminal procedure is concerned, searches, seizures and demands for the production of data sets must still comply with the traditional provisions for physical objects, which do not take account of many of the particularities of data. In contrast to the request for production of tangible objects, when seeking coercive access to data for investigation purposes, the state must consider the possibility of making a copy of the data (instead of confiscating the physical data storage media), of the need to oblige witnesses to express encrypted data as plain text or – even more invasively – to divulge or hand over passwords and access keys that afford investigating authorities unlimited access to the information system. If e-mails are seized from the e-mail provider, it must be determined whether the data have already been received by the recipient and are thus covered by the broader seizure provisions or whether it will be necessary to interfere in an ongoing transmission, in which case the significantly stricter provisions governing telecommunications surveillance apply.

The current practice of covertly gaining access to computers communicating with each other and capturing data from the still encrypted source while invoking the regulations on telecommunications surveillance is questionable and – according to the findings of the Institute in Freiburg – unconstitutional. Such "surveillance of telecommunications data at the source" in fact constitutes a "small" online search, a procedure that is not foreseen in the Code of Criminal Procedure (legislation that governs the repressive activities of criminal prosecution) – in contrast to the Act on Danger Prevention (legislation that regulates the proactive measures of the Federal Criminal

Police). Indeed, the Federal Constitutional Court has called for special legal and technical protective measures for this type of search. However, these special provisions are not included in the current act on telecommunications surveillance. In order to draft new regulations, it will be necessary to clarify, for example, whether the exchange of data with a cloud provider represents a "telecommunication," which can be intercepted by law enforcement using the provisions of telecommunications surveillance, or whether from a functional perspective it is just an instance of communication with one's own data, which could only be intercepted by means of a "large" online search – currently unavailable in the context of criminal prosecution. To date, this problem – like numerous other issues identified in one of the Institute's recent publications – has not even begun to be addressed in the case law or in the legal literature.

Nor have the questions resulting from the global nature of cyberspace been resolved; for example, the extent to which investigating authorities may act on foreign servers via the worldwide Internet is largely unclear. The prevailing opinion is that this violates the sovereignty of the state in which the server is physically located, at least as far as non-public information is concerned. If these regulations are taken seriously, if no new solutions are found for legal and administrative cooperation and if no new law enforcement institutions for cyberspace are created, major problems can be expected to arise soon. This is especially true for cloud computing, as it is often not clear – even to the participants themselves – where in the global cloud, that is, on whose territory, the sought-for data are actually located.

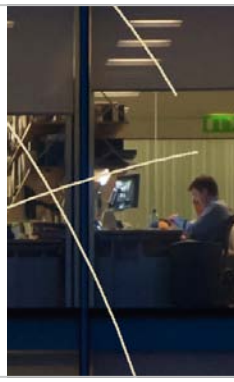
As stated in the expert opinion prepared by the Freiburg Institute and elsewhere, the failed attempts to block online child pornography have clearly shown that old concepts of protection, consisting in walling off the nation-state from foreign territories, are long since unworkable on the Internet. Thus, the traditional concepts of sovereignty, territoriality and administrative and legal cooperation are subject to a fundamental challenge when enormous quantities of data in the Internet are moved around the world in mere milliseconds. Here, too, the traditional rules governing the border control of physical objects are doomed to failure, and new solutions are called for.

IMPLEMENTING THE RESULTS IN LEGAL POLICY

The basic research conducted at the Institute in Freiburg contributes in myriad ways to the solution of practical problems. This transfer of research results into current legal policy can be seen, for example, in the hearings before the German Federal Constitutional Court on online searches (computer surveillance), the deliberations of various parliamentary committees on Internet blocking and on the preventive offenses of terrorist propaganda, the vote of the Council of Europe on preventing cyber terrorism and the newly begun efforts at the United Nations to develop global legal standards in the area of cybercrime. The proposals for a comprehensive reform of the German criminal law of information recently prepared by the Freiburg Institute will form the basis of deliberations at the next conference of the Association of German Jurists in Munich in September 2012.

These activities, driven by fundamental ideas and guided by theory, clearly illustrate how helpful the results of basic research can be for practical questions in the legal sciences. Conversely, basic research that is open to practical questions profits from a multitude of stimuli. The development of information law in cyberspace supports the physicist Max Planck, who stated, "Knowledge must precede application." Furthermore, it confirms the phrase attributed to the philosopher and jurist Immanuel Kant: "There is nothing more practical than a good theory."

THE INSIGHT STEMMING FROM CYBERNETICS THAT INFORMATION IS NEITHER MATTER NOR ENERGY, BUT A THIRD "BASIC VARIABLE" IS AN IMPORTANT REMINDER FOR LEGAL SCIENCE, TO CHALLENGE THE WAY IN WHICH INFORMATION LAW-RELATED PROBLEMS ARE STILL LARGELY SOLVED, NAMELY, BY APPLYING THE RULES DEVELOPED FOR PHYSICAL OBJECTS



Literature

Ulrich Sieber, Straftaten und Strafverfolgung im Internet – Welche Maßnahmen empfehlen sich im Hinblick auf die neuen Herausforderungen der globalen Informationsgesellschaft?, Ständige Deputation des Deutschen Juristentages (ed.), Verhandlungen des 69. Deutschen Juristentages, Munich 2012, pp. C 1 – 148.

Id., Mastering Complexity in the Global Cyberspace, in: Mireille Delmas-Marty/ Mark Pieth/ Ulrich Sieber (ed.), Les chemins de l'harmonisation pénale, Paris 2008, pp. 127 – 202.

Id., Rechtliche Ordnung in einer globalen Welt, Rechtstheorie 41 (2010), pp. 151–198 (English translation: Legal Order in a Global World, in: A von Bogdandy / R. Wolfrum, eds., Max Planck Yearbook of United Nations Law vol. 14, 2010, pp. 1 – 49.