Sicherheitspolitische Gesamtbetrachtung der Hochschulen in einem vernetzten Europa

Katharina von Knop

Leopold-Franzens-Universität Innsbruck

Zusammenfassung Der Einsatz des Internet entwickelt sich trotz des wirtschaftlichen Einbruches im dot.com Markt und der Ereignisse vom 11. September in allen Teilen unserer Gesellschaft, Wirtschaft und Wissenschaft unbeirrbar fort. Die neuen Möglichkeiten der Internet-Technologie beinhalten schwierige Herausforderungen an die politische und wirtschaftliche Führung unserer Länder, sowie an unsere Selbstverwaltungsgremien in der Wissenschaft.

Es stellen sich immer neue Fragen, ob die neuen Netzwerktechnologien einen weiteren Regelungsbedarf seitens unserer Regierung bedürfen und insbesondere welche Schutzbedürfnisse sich daraus ergeben und welche Schutzmaßnahmen notwendig sind. Aufgrund des Fehlens einer globale Regierungs- oder Regulierungsbehörde, ist die Behandlung der politischen Gesichtspunkte auf der globalen Ebene besonders schwierig.

Gerade die europäischen Hochschulen sind als Institutionen der Forschung und Lehre in einem vernetzten Europa gefordert neue Technologien zur Sicherung der Netzwerksysteme zu entwickeln, um den Schutz hochsensibler Daten zu gewährleisten. Es ist gerade die Asymmetrie der heutigen Konflikte die unsere Gesellschaften gefährden können. Um diesen Bedrohungen effektiv entgegen zutreten ist eine verstärkte Zusammenarbeit der europäischen Hochschulen auf technologischer und auch politischer Ebene unerlässlich.

Das Kernelement der Politikwissenschaft ist unter Betrachtung der Theorie der internationalen Politik des Realismus von Hans Morgenthau der Begriff Macht. Oberste Priorität hat deswegen die Aufrechterhaltung und Sicherung der Macht und das ist, wie uns die jüngste Geschichte drastisch vor Augen geführt hat um ein vielfaches schwieriger geworden.

Was als Bedrohung von Sicherheit empfunden und wahrgenommen wird hat sich einer Veränderung unterzogen. Heute steht nicht mehr der Angriff auf ein Territorium eines Staates in Vordergrund, sondern auf sein System, seine Gesellschaft, seine Symbole, das Funktionieren seiner Institutionen und das Wohlergehen seiner Bürger. Die Sicherheitsrisiken sind vielfältiger und diffuser geworden. Die Grenzen zwischen zivilen und militärischen Risiken lösen sich zunehmend auf. Die Angriffe sind asymmetrisch und die Aggressoren sind schwer zu identifizieren.

Die Ursachen der Bedrohung liegen nach Professor Pelinka [1] auch in der Gesellschaft des eigenen Landes. Gesellschaften haben allerdings nicht nur nationalstaatlichen Grenzen, sondern auch ökonomische, kulturelle und ethische.

Diese Feststellung gilt insbesondere für unsere Hochschulen, die nicht nur in nationalstaatliche Bildungssysteme eingebunden sind, sondern in ein europäisches oder eher globales.

Diese Grenzenlosigkeit hebt einerseits damit den Unterschied zwischen innerer und äußerer Sicherheit auf, andererseits sind innere und äußere Sicherheit voneinander abhängige Faktoren. Das bedeutet für die europäische Sicherheit, dass die Erweiterung und die zunehmende Integration der EU einen Beitrag zur europäischen Sicherheit darstellt, so Professor Pelinka.

Isolierte nationalstaatliche Systeme im Bereich der hard security, wie z.B. das Amerikanische Raketenabwehrsystem NMD stellt nach Auffassung von Politikwissenschaftlern [1] keinen Beitrag zur globalen oder europäischen Sicherheit dar.

Der transnationale Charakter der meisten aktuellen Risiken erfordert in der Sicherheitspolitik internationale Zusammenarbeit bei der Früherkennung, Prävention und Krisenbewältigung. Das effiziente Zusammenspiel verschiedener Instrumente der Macht, d.h. im Bereich der hard powers, Elemente wie Militär und Wirtschaft und im Bereich der soft powers, die Attraktivität des eigenen Systems und die Fähigkeit die internationale Politik zu beeinflussen ist notwendig Dies ist Vorraussetzung für ein effektives Krisenmanagement und basiert wesentlich auf den neuen Informationstechnologien.

Im 21. Jahrhundert werden sich die Beherrschung der Informations- und Kommunikationstechnologien sowie die Befähigung zur Bestimmung der Informationsinhalte zu den wichtigsten Machtfaktoren in den internationalen Beziehungen entwickeln. In der Informationsgesellschaft lösen Technologie, Information, Bildung und institutionelle Flexibilität die traditionellen Faktoren Raum, Arbeitskräfte und Rohstoffe als strategische Ressource ab. Information und Kommunikation werden im Rahmen der steigenden Bedeutung von soft power zu strategischen Faktoren.

Sie sind jedoch nicht per se eine Quelle von Macht. Im Zeitalter der elektronischen Medien ist öffentliche Information ein knappes Gut . Sie zu verbreiten ist einfach und billig geworden, es gibt Informationen im Überfluss. Knapp hingegen ist Aufmerksamkeit, die den riesigen Informationsfluss entgegengebracht wird. Das Hauptproblem ist nicht die Beschaffung sondern die Filtrierung und Reduktion von Information. In diesem Kontext ist Glaubwürdigkeit die kritische Ressource zur Herstellung von Aufmerksamkeit in der Informationsgesellschaft .

Wie glaubwürdig ist in diesem Kontext die Sicherheit Europas?

Der Wandel vom alten System zur Informationsgesellschaft zeichnet sich deutlich in der Wahl der Objekte ab. Je wichtiger die digitale Datenübertragung – und Speicherung für den Ablauf administrativer Prozesse wird, desto interessanter ist es für Terroristen diese zu sabotieren. Wie empfindlich und verwundbar unsere Gesellschaft ist, zeigte sich nur zu deutlich in den sekundär und tertiär Folgen des 11. September.

Die Schäden, die durch Missbrauch und Störungen durch Hacker und Viren unserer Gesellschaft entstehen sind gewaltig. Der im Jahr 2000 verbreitete Pseudoliebesbrief „I love you“ hat mit 8,75 Milliarden Dollar bislang von allen Computerviren die höchsten Kosten verursacht. Dies geht aus einer Untersuchung von Computer Economies Inc. aus Carlsbad bei San Diego (US-Staat Kalifornien) hervor. Der von kriminellen Hackern versendete Wurm „Code Red“ kostete die Unternehmen insgesamt 2,62 Milliarden Dollar und liegt damit auf Platz zwei. Dahinter rangiert „Melissa“. Der 1999 aufgetauchte Schädling pulverisierte 1,1 Milliarden Dollar.

Es ist evident, dass die ohnehin sehr schwach finanzierten Hochschulen in Europa an diesen Schäden und den daraus folgenden Kosten maßgeblich partizipieren.

Was dürfen nun die Hochschulen in diesem Kontext erwarten?

Die Europäische Kommission im Jahre 2001 einen Vorschlag zur Bekämpfung Computerbezogener Verbrechen veröffentlicht. Das Dokument enthält keine konkreten gesetzgeberischen Vorschläge, skizziert aber in groben Zügen, wie sich die Kommission die Bekämpfung von Cyberkriminalität vorstellt. Ein Europäisches Forum, bestehend aus Strafverfolgungsbehörden, Telekommunikations-Service-Providern, Konsumentengruppen und Datenschützern, soll die Kooperation auf europäischer Ebene verstärken. Der Vorschlag der Europäischen Kommission mit dem Titel „Creating a Safer Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime“, stellt fest, dass effektives Handeln zur Bekämpfung von High-Tech-Kriminalität auf nationaler und internationaler Ebene nötig seien, da solche Verbrechen im grenzenlosen Cyberspace sich nicht an die Staatsgrenzen halten würden [2].

Im April 2002 folgten neue Vorschläge der Kommission, da es nach Auffassung des Kommissars Antonio Vitorine inzwischen eindeutige Hinweise auf Beziehungen zwischen organisierter Kriminalität und den Internetangriffen gibt. Der Gesetzentwurf, den die Presse mit „Europe plans to jail Hackers“ apostrophierte, sieht als Mindeststrafe 1 Jahr Gefängnis für cybercrime, und vier Jahre für Angreifer, die einen wirtschaftlichen Schaden anrichten. Das größte Problem stellt aber die Harmonisierung dieses Gesetzentwurfes mit den bereits existierenden nationalen Gesetzen der 15-Länder EU dar.

Das Informationszeitalter führte neben den neuen Möglichkeiten der Informationsversorgung und der vielen neuen Comodity Services auch zu einem asymmetrischen Verhalten und Auswirkungen von künftigen Konflikten. Diese Asymmetrie wird besonders deutlich vergleichen wir die Kosten - Nutzen Relation. Heutige Hochleistungswaffensysteme kosten ein bis dreistellige Millionenbeträge, pro Einheit und können auch vergleichbare Schäden verursachen.

Ein einzelner Hacker kann dagegen heute Millionenschäden produzieren wie der „I love you“ -Virus gezeigt hat [3]. Arnauld Borschgrave vom Center for Strategie International Studies „Mit sehr exzellenten Hackern und zehn Millionen Dollar kann man die USA in die Knie zwingen“ [4]. Gleichwohl kann man solchen Aussagen nicht unkritisch gegenüber stehen oder sie gar in die Nähe einer Interessensverfolgung bringt, so zeigen sie dennoch auf das zunehmende Ungleichgewicht zwischen den eingesetzten Mitteln und die Auswirkung hin.

Die Aussagen europäischer Politiker sind dagegen deutlich verhaltener oder nehmen gar beschwichtigende Form an. So bezeichnet der oberste Brandenburgische Verfassungsschützer Heiner Wegesin [5] die nach dem 11. September auch in Deutschland verstärkt diskutierte Gefahr eines bevorstehenden Cyberterror-Anschlags [6] als deutlich überhöht. Es lägen nach seiner Kenntnis „der Geheimdiensten – auch internationalen“ keine Anhaltspunkte vor, dass die virtuelle Dimension als eine der Methoden zum Einsatz kommen soll, die den Terrorismus bedingen“. Damit spielt der Verfassungsschützer der Cyberkomponenten bei der Frage des Terrorismus an den weltweiten Brandherden auf, „eine absolute

Randrolle herunter und weicht mit dieser Einschätzung vom üblichen Alarmismus [7] seiner Branche ab.

Nicht so optimistisch sieht die Bedrohungslage in Deutschland der Arbeitskreis Schutz von Infrastrukturen AKSIS [8]. Demnach gäbe es zwar in Deutschland keine reale Bedrohungslage, aber aufgrund des hohen Vernetzungsgrades der Bereiche wie Flugsicherung, Elektrizitätsversorgung, Wasserversorgung seien die „Tatgelegenheitsstrukturen“ sehr ernst zu diskutieren.

Dass unser Bildungssystem nicht nur von den täglich stattfindenden Hackerangriffen betroffen ist, sondern durchaus auch größere Schäden erleiden kann, zeigte sich am Beispiel der Pace University, New York, die nach dem 11. September erhebliche kollaterale Schäden erlitten hatte [9]. Obwohl die Universität nicht das Ziel des terroristischen Angriffs war, wurde in deren Gebäude die Strom- und Wasserversorgung, die IT-Infrastruktur, sowie die im World Trade Center untergebrachten Internet-Server unterbrochen bzw. zerstört. Aufgrund eines „disaster recovery plans“ für die IT, den die Pace University bereits vor 2 Jahren zu implementieren begonnen hat und der redundanter Backbone, und backup facilities in einem anderen Stadtteil beinhaltete waren die IT-Ausfälle erträglich.

In diesem Zusammenhang drängt sich natürlich die Frage auf, wie abhängig sind europäischer und insbesondere deutscher Hochschulen von den verfügbaren Informationstechnologie? Und wieweit sind die Hochschulen, aufgrund ihrer permanenten Unterfinanzierung gegen Ausfälle ihrer IT-Infrastrukturen abgesichert.

Ein direkter Vergleich hinsichtlich der Verwundbarkeit europäischer und amerikanischer Hochschulen ist aufgrund der unterschiedlichen politischen Rahmenbedingungen und der Bildungsstruktur nicht ohne weiteres möglich.

Während sich in USA bereits die ersten Organisationen formiert haben, die sich mit der Bedrohungsanalyse, der gemeinsamen Vorbereitung von Schutzmaßnahmen und Warnung aktiv betreiben, hat die EU Kommission erst begonnen, sich damit zu befassen. So hat das FBI bereits 1999 das „National Infrastructure Protection Center“ gegründet, welches die internationalen Bedrohungen aus dem Internet verfolgt [10].

Als Grund für das höhere Schutzbedürfnis der US amerikanischen Infrastrukturen vor Internet-Attacken wird die starke Abhängigkeit von Computernetzwerken angeführt. So hat die „Presidential Commission an Critical Infrastructure Protection“ (PCCIP) bereits am 13.10.1997 ihren Abschlussbericht „Critical Foundations“ vorgelegt.

Der Geschichtsprofessor Paul Kennedy und Direktor des „International Security Studies Program“ in Yale tritt für die dringend notwendige Verbesserung des Geheimdienstes ein und mahnt eine enge Zusammenarbeit der Politik mit den Universitäten und der Wirtschaft [11].

Die heutige strategische Macht der USA beruht auf einem unvergleichlich soliden technisch-wissenschaftlichen Fundament. Gut 40 Prozent des gesamten Internetverkehrs spielen sich in den USA ab, und knapp drei Viertel aller neueren Nobelpreisträger arbeiten an Universitäten und Laboratorien in den USA.

Durch ihre Forschungsergebnisse und Wissenschaftler, die sie ausbilden, reproduzieren sie die wichtigsten Quellen der amerikanischen Stärke und Wettbewerbsfähigkeit. Dadurch

verfügen die USA über die notwendigen materiellen, intellektuellen und militärischen Ressourcen, um ihre Machtposition gegenüber der internationalen Staatenwelt aufrechtzuerhalten.

Macht entsteht heute also über ein Zusammenwirken verschiedener Machtinstrumente. Dennoch wird es den USA schwer fallen, einen zweigleisigen klassischen Kampf und einen dezentralisierten mit nichtmilitärischen Mitteln geführten Cyberkampf zu führen.

Durch internationale Netzwerke, d.h. die Schaffung von Network Powers als Partizipationschance der europäischen Staaten kann ein verstärktes Maß an Sicherheit durch Kooperation gewonnen werden.

Was für Schlüsse sollen Europäer nun aus diesen vielen Stimmen ziehen, insbesondere im Hinblick auf die Sicherung unserer informationstechnischen Infrastrukturen?

Zum einen ist weder der Globalisierungsprozess noch der Einsatz des Internet in unserer Gesellschaft umkehrbar. Zum anderen müssen die Europäer ihre Ressourcen intellektueller, wirtschaftlicher, technischer und diplomatischer Art, von denen sie wirklich genügend haben, bündeln.

Eine zentrale Rolle spielen dabei natürlich die Hochschulen. Wir müssen uns auf unsere Geschichte besinnen und uns wieder bewusst machen, dass die Errungenschaften der Wissenschaft zum wirtschaftlichen Wohlstand unserer Länder führten und das die Hochschulen nicht nur die Instrumente einer Regional- und Steuerpolitik sein dürfen.

Die Hochschulen müssen, um in einem zunehmend sicherheitsorientierten Internet nicht nur den an sie gerichteten Erwartungen gerecht zu werden, sondern ihrem Selbstverständnis als Vorreiter der Entwicklung Rechnung zu tragen und folglich Antworten auf grundlegende sicherheitspolitische Fragen entwerfen (s.a. [12]).

Der Aufgabenkatalog, an dem sich in den kommenden Jahren die Hochschulen messen lassen müssen.

1. Von den Hochschulen dürfen keine Angriffe ausgehen.
   Die Freiheit von Wissenschaft und Lehre erfordert liberale Regelungen für den Zugang aus der Hochschule zum Internet. Dennoch dürfen die beträchtlichen Rechenkapazitäten und schnellen Internetanbindungen der Universitäten nicht dazu missbraucht werden, Denial-of-Service-Angriffe und andere bösartige Aktivitäten auszuführen, oder auch nur vorzubereiten oder zu koordinieren.
2. Angriffe innerhalb der Hochschulen müssen unterbunden werden.
   Dies ist nicht nur notwendig, um die Funktionsfähigkeit der Hochschule zu erhalten, sondern es gibt auch vielfältige sensible Daten, wie z.B. medizinische Patientendaten, Prüfungsaufgaben, Forschungsergebnisse oder Patentschriften, die zuverlässig vor unberechtigtem Zugriff geschützt werden müssen.
3. Hochschulübergreifende Kooperationen in Fragen der IT-Sicherheit sind unabdingbar.
   Universitäten müssen ihre Sicherheitskonzepte, ihre Erfahrungen und organisatorische Maßnahmen untereinander austauschen, und zwar nicht nur auf nationaler, sondern auch auf europäischer Ebene, zumal mit dem Fortschreiten der europäischen Einigung sich auch die gesetzlichen und wirtschaftlichen Rahmenbedingungen angleichen, unter denen die Universitäten operieren.

Wenn es dabei zur Entwicklung allgemein anerkannter Standards oder „Best Practices“ kommt, kann dies nur hilfreich sein, ebenso wie ein Austausch aktueller Informationen über Schwachstellen und akute Bedrohungen.

4. Hochschulen müssen hinsichtlich der Ausbildung des IT-Personals und der IT-Anwender Standards setzen.

   Die anstehenden Sicherheitsprobleme können nur bewältigt werden, wenn die Mitarbeiter ausreichend qualifiziert und besonders in Fragen der IT-Sicherheit geschult sind.

   Dies bedeutet nicht nur, dass das IT-Personal in der Lage ist, Sicherheitsprobleme zu erkennen und zu lösen, sondern dass auch die Anwender der IT über die Gefahren und Risiken des Computereinsatzes in ihrem Arbeitsbereich informiert sind und insbesondere ein angemessenes Sicherheitsbewusstsein entwickeln.

   Die Hochschulen, zu deren Hauptaufgaben nun einmal die Ausbildung gehört, sollten Anforderungskataloge und Schulungsprogramme für die IT-Sicherheit entwickeln und bei deren Umsetzung mit gutem Beispiel vorangehen.

5. Die Forschung muss sich verstärkt mit der Entwicklung hochsicherer und vertrauenswürdiger Systeme befassen.

   Damit die allzu zahlreichen Verwundbarkeiten der heute eingesetzten Software bewältigt werden, ist weitreichende Forschungsarbeit notwendig, die jene Voraussetzungen für den praktischen Einsatz sicherheitstechnisch zuverlässiger Computersysteme und Kommunikationsprotokolle schafft.

   Es wird den politischen Instanzen vorbehalten bleiben, die Rahmenbedingungen für eine Finanzierung solcher Forschungsarbeiten zu schaffen und Anreize für eine Realisierung sicherer Systeme und Netzwerke zu geben.

6. Die Mechanismen des Internet müssen sicherer werden.

   Viele der heute verwendeten Steuerungsmechanismen des Internet z.B. die Nameserver und das Routing wurden ursprünglich auf ihre Funktionalität hin und nicht unter Sicherheitsaspekten entwickelt. Den Hochschulen kommt einerseits die Aufgabe zu, im Rahmen der Forschung an einer Verbesserung dieser Mechanismen zu arbeiten, und andererseits in ihren Netzwerken innovative Lösungen zu erproben. Insbesondere für die letztgenannte Aufgabe sind sie prädestiniert, können sie doch einen umfassenden Erfahrungsschatz, komplexe Netzwerkstrukturen und ihre Fähigkeit zu internationaler Kooperation einbringen.

7. Die Sicherheit neuentwickelter Technologien und Systeme muss bereits beim Design vorrangig berücksichtigt werden.

   Gerade bei der Entwicklung der Funknetzwerke zeigt sich, dass für die kommerziellen Anbieter, die mit neuen Technologien den Markt erobern wollen, die Funktionalität und leichte Bedienbarkeit wichtigere Marketingargumente darstellen, als eine inhärente Sicherheit. Hochschulen können sich, leichter als der private Sektor, technologischen Modetrends verschließen, wenn diese sich als unsicher erweisen, und stattdessen sowohl in der Forschung als auch im praktischen Einsatz auf Lösungen setzen, die auch in der vorhersehbaren Zukunft eine ausreichende Sicherheit gewährleisten.

   Es hat sich in der Vergangenheit oft gezeigt, dass Systeme, die von der Industrie als sicher genug angesehen wurden, um in den Rechenzentren und Netzwerken großer

Firmen ihren Dienst zu tun, an Universitäten kläglich versagten, weil sie den kreativen und beharrlichen Angriffen von Seiten der Studierenden nicht standhielten.

8. Der Persönlichkeitsschutz der Nutzer muss gewahrt bleiben.
   Hierzu gehört nicht nur der Schutz der nutzereigenen bzw. nutzerbezogenen Daten, sondern auch die Wahrung der Anonymität der Nutzer, soweit dies jedenfalls möglich ist, ohne dass strafrechtliche Normen verletzt werden.

Gerade im Hinblick auf die schon bald zu erwartende Vielzahl mobiler Geräte, die untereinander und mit stationären Systemen selbständig in Verbindung treten und Daten austauschen, steht zu befürchten, dass Daten, Bewegungs- und Handlungsprofile von Personen in solchem Umfang erfasst werden, dass die Freiheits- und Persönlichkeitsrechte verletzt werden. Dies darf an einer Hochschule nicht geschehen, gleichgültig, ob die Person zu den Professoren oder den Studierenden zählt.

Literatur

[1] Anton Pelinka, Die Ambivalenz von äußerer und innerer Sicherheit in „Wie sicher ist Europa - Perspektiven einer zukunftsfähigen Sicherheitspolitik nach der Jahrtausendwende“, 17. Internationale Sommerakademie Österreichisches Studienzentrum für Friedens- und Konfliktforschung, 9.-16.7.2000
http://www.aspr.ac.at/asprivie/sak2000htm

[2] http://www.19.4.2002gcn.com/cybersecurity

[3] Reinhard Kutter, Risiken im Informationszeitalter in „Sicherheitspolitik in neuen Dimensionen“, Verlag E.S. Mittler & Sohn GmbH, Seite 483-500 (2001)

[4] „Krieg im Computer“, in Die Zeit Nr. 2, 05.01.2000

[5] http://www.Verfassungsschutz-Brandenburg.de

[6] Heinz Heise, Verfassungsschützer gibt Entwarnung beim „Cyberterror“

[7] http://www.heise.de/neusticker/data/jb-06.01.02-0003/

[8] http://www.aksis.de

[9] Frank J. Monaco, IT-Disaster Reovery Near the World Trade Center. EDUCAUSE Quaterly 4, S. 4-7 (2001)

[10] Infra-Gard-Initiative und Information Technology Information sharing and Analysis Center

[11] Paul Kennedy, Die Bewahrung der amerikanischen Macht in „Das Zeitalter des Terrors“, S. Talbott und N. Chanda (Hrsg.), Propylen 2002

[12] A National Strategy to Secure Cyberspace; Questions to be Adressed. Government Computer News, 19. April 2002