erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

FIfF-Konferenz 2016

CYBER! Der Staat als Krimineller

Zusammenfassung des Vortrags von Erich Möchel

Nach Stuxnet, Duqu, oder Zeus und Black Energy, nach dem Re-Engineering des Bundestrojaners und den Enthüllungen Edward Snowdens über den massiven Einsatz hochentwickelter Schadsoftware durch NSA und GCHQ ist klar, dass hier ein neuartiger Rüstungswettlauf außer Kontrolle geraten ist.

Erich Möchel hat seit 1995 lebhaft mitverfolgt, wie Staaten sich selbst trotz ihrer eigenen Verbote das Recht einzuräumen begannen, Schadsoftware einzusetzen. In seinem geschichtlichen Abriss über die Entwicklung wird das erschreckende Ausmaß deutlich: Staaten der westlichen Demokratien hätte auch er nicht für so skrupellos gehalten, zu allen verfügbaren Mitteln zu greifen.

Etymologische Bemerkungen zu dem Begriff *Cyber*

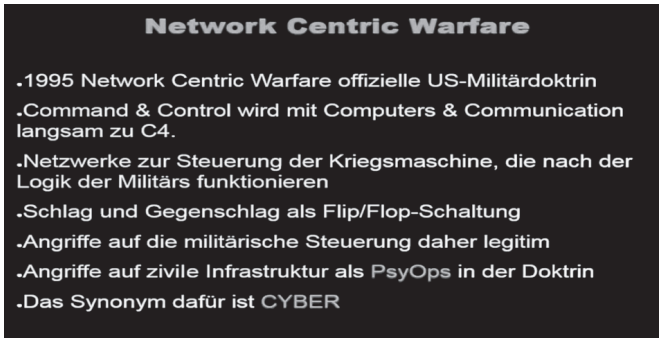
Cyber ist ein Begriff, der sehr viel unter sich subsumiert. Er wurde ursprünglich vom Staat beansprucht und beschrieb immer eine staatliche Aktion. Die ältesten Anwendungen des Wortes standen für Lenkung, Steuerung – für den Staat. Bei Homer ist der κυβέρνητης der Schiffssteuermann und auch in dem Wort Κυβέρνησις, wie die Regierung im alten Athen hieß, ist das Wort *Cyber* versteckt. Im Mittelalter ist daraus dann der Gouverneur – ein Militärbefehlshaber – geworden. 1948 prägte Norbert Wiener den Begriff *Cybernetics* für Steuerungs- und Regelungskunde, Maschinen, Organismen und soziale Organisationen. Der Begriff wurde daraufhin sehr breit angewendet. Im Zuge des Behavioristischen Modells der Psychologie, das damals langsam entstand, dachte man, man könnte alles lenken und gesellschaftliche Vorgänge nach Belieben manipulieren. Die Sowjetunion ist daran zugrunde gegangen, aber diese Art des Denkens war im Westen fast noch verbreiteter.

Der Begriff Kybernetik tauchte dann überall in der Wissenschaft auf: Claude Shannons Informationstheorie, bei Paul Watzlawick, bei Maturana/Varela bis zur Systemtheorie Niklas Luhmanns.

In den 60er-Jahren gab es sogar eine Kybernetische Pädagogik. Man nahm den Begriff wörtlich und wendete ihn auf alle Bereiche der Gesellschaft an. Einzug in die Gesellschaft selbst erhielt der Begriff in den 80er-Jahren, als die Alternativen zum ersten Mal nach dem Begriff griffen und die *Cyberpunk Fiction* schufen. Zu Ehren kam der Begriff *Cyber* schließlich in der *Cybercrime Convention* im Europarat (COE), als der Europarat, der sich sonst mit Menschenrechten beschäftigt, im Bereich *Cyber* Überwachungsgesetze beschloss, da „man ja alle möglichen Menschen vor dem Netz schützen muss".

Network Centric Warfare

Seit 1995 ist *Network Centric Warfare* die offizielle US-Militärdoktrin. Dies ist kein Geheimwissen und nicht unsichtbar, sondern wurde als Konzept des vernetzten Krieges festgeschrieben. *Command & Control Center* – die Gefechtsfeldzentralen – wurden erweitert um *Computers and Communication* und wurden langsam zu C4 (*Command, Control, Computer and Communication*). Die Kontrolle der Kommunikation wurde also zur üblichen Gefechtszentrale (das sind im Wesentlichen die Systeme, die jede Armee der Welt verwendet) einfach hinzugefügt. Die so entstandenen Netzwerke funktionieren nach der Logik der Militärs. Diese Logik ist unerbittlich: Schlag und Gegenschlag. In dem Moment, in dem man das Gebiet der Militärlogik betritt, gelten all unsere Regeln nicht mehr. Es gilt auf diesem Gebiet nur noch das furchtbare Gesetz des Krieges. Schlag und Gegenschlag wurden eingeplant wie eine Flip-Flop-Schaltung in der Elektronik. Wie zwei Transistoren, die sich gegenseitig ein- und ausschalten. Das Prinzip selbst galt aber beim Militär schon länger; selbst Angriffe auf die militärische Steuerung sind daher eine ganz legitime Handlung. Es war nur die Frage, zu welchem Zeitpunkt man den *Cyber*-Angriff starten kann und vor allem,



wie er von der Gegenseite eingeschätzt wird und wie diese darauf reagiert.

Angriffe auf die zivile Infrastruktur waren schon vorher als sogenannte PsyOps – Psychologische Operationen – Teil der Doktrin der Militärs. Derartige militärische Aktionen waren eine dem Schießkrieg vorgelagerte Art des Handelns und der gegenseitigen Schlagabtausche, zu denen z. B. auch Propaganda und somit Kommunikationsmedien und Breitenmedien gehören. Als weitere Stufe folgen dann aber auch direkte Angriffe auf Websites und Informationssysteme. Im Irak konnte man das 2003, kurz vor Einmarsch der Amerikaner, täglich verfolgen: Von einem Tag auf den anderen wurden plötzlich sämtliche irakischen Regierungswebsites gehackt. Die Amerikaner haben diese Angriffe eher unglaubwürdig, aber umso heftiger dementiert. Die Websites waren zwar miserabel gehostet, es konnte aber nicht sein, dass es sich bei dieser Gleichzeitigkeit um eine Vielzahl von Einzelaktionen handelte. Nachdem all diese Websites lahmgelegt waren, wurden die Radio- und Fernsehausstrahlungen im Irak angegriffen. Auch in diesem Bereich ist also *Cyber* angesiedelt; all diese Aktionen passieren im Vorfeld des Schießkrieges und inwiefern das vom tatsächlichen Krieg abzugrenzen ist, ist nicht festgelegt. *Cyber* dient als Synonym für all diese unsinnigen militärischen Aktionen. Er steht für alles: für Angriffe mit Mitteln der Kommunikation auf die Kommunikation, Angriffe, die keine herkömmlichen Waffen beinhalten und die nur sehr schwer zuzuordnen sind. In dieser ersten Phase des Angriffs bleibt der Angreifer unsichtbar – ein Musterbeispiel für ein *invisible system*, bis zu dem Punkt, an dem der Angreifer sich im Netzwerk des Gegners befindet und dort auffällt.

Die sogenannten Cryptowars

Ein hierzu passendes *Invisible Office* findet man in Wiens erstem Bezirk in der Mahlerstraße 14. Dieses *Wassenaar Office*, das seinen Namen vom sogenannten *Wassenaar Arrangement* bekam, beschäftigt sich mit *Cyber*, Schadsoftware und Crypto. Das Büro ist eigentlich niemandem bekannt, aber wichtig, denn es verwaltet die Nachfolge der CoCom-Listen, jenes Verfahren, mit dem sich die westlichen Staaten verpflichteten, keine Hochtechnologien an die Sowjetunion zu liefern, also Embargolisten. Das *Wassenaar Office* hat ebendies fortgeführt: Sie führen ordentliche Kataloge von Waffentechnologie, und was als Waffe verstanden wird, ist dort definiert. Darunter zählen z. B. Funkscanner, die mehrere Frequenzen gleichzeitig scannen, Geräte mit Technologien, die jenseits der 31 GHz operieren – im Prinzip die gesamte Palette an Dual-Use Goods – die vielen Güter also, die man sowohl in der Zivilgesellschaft als auch im Krieg benutzen kann. Der Konflikt der 90er-Jahre um das freie Bereitstellen von Verschlüsselungsprogrammen ist nun unter dem Begriff *Cryptowars* bekannt. Journalist.innen und die technikinteressierte Zivilgesellschaft haben das nie so genannt, und es vergingen viele Jahre, bis dieser Begriff überhaupt als Militärbegriff bekannt wurde.

Die österreichische Bundesregierung hatte sich noch nicht festgelegt, wie sie zu Kryptografie stand, wusste das Thema eigentlich auch noch gar nicht richtig einzuschätzen, konnte aber nicht wirklich etwas dagegen einwenden, da es auch in Österreich etwa ein Bankgeheimnis gab. An dieser Stelle nur ein ganz kurzer Abriss über die Eckdaten: 1976 begann die ideelle akademische Befreiung von Kryptografie, denn bis dahin hatten nur die Militärs Zugang zu den Fachbüchern. Whitfield Diffie und Martin Hellman befreiten Kryptosysteme 1976 aus Militärhaft, indem sie Kryptografie auf der Konzeptebene re-engineerten. 1991 stellte Phil Zimmermann PGP als Commandline-Version ins Netz und erhielt daraufhin Besuch vom FBI, wobei zu sagen ist, dass in der frühen Zeit des Netzes viele erst einmal „gemacht" haben, ob legal oder illegal war damals noch keine relevante Frage. Der Leak der OECD-Kryptobestimmungen durch den österreichischen Datenschutzverein *Quintessenz* schlug im Hintergrund diplomatische Wellen. 1994 führte Netscape SSL 1.0 als Kryptografiestandard ein, was für Banken von höchstem Interesse war, da Menschen nun selbst ihre Konten führen, Arbeitsplätze abgebaut und Filialen geschlossen werden konnten – was dann auch genauso geschah.

1995 wurde Kryptografie auf Betreiben der USA im *Wassenaar Arrangement* zu Munition. Jemand, der Verschlüsselungsanwendungen geschrieben hatte oder Software und Verschlüsselungshardware baute, durfte diese nicht ohne Genehmigung der eigenen Regierung exportieren. Wenn das Zielland nicht als Empfänger erwünscht war, wurde diese Genehmigung nicht erteilt. Kryptografie, welche ihrem Wesen nach rein defensiv eingesetzt wird, wurde damals als offensive Waffe eingestuft. Aus diesem Grund konnten Netscape und Microsoft keine sichere Verschlüsselung einbauen, weil sie nicht garantieren konnten, dass ihre Software nur in genehmigten Ländern heruntergeladen wird.

Die Banken hatten jedoch nach wie vor ein erhebliches Interesse an sicherer Kryptografie, und so entstand sehr plötzlich eine ungewöhnliche Allianz mit den zivilen Technik-Communities. „Banken, die E-Commerce betreiben wollten, taten sich zusammen mit solchen Narren wie uns", beschreibt Möchel. In einer weltweiten Allianz im Rahmen der *Global Liberty Campaign* hatten sich auch die American Civil Liberties Union, die Electronic Frontier Foundation und viele kleine europäische Gruppen, die sich gerade erst gebildet hatten, zusammengefunden. Zu dieser Zeit wurde heftig über die Zukunft der Kryptografie diskutiert. Die sogenannten *Spooks* wussten längst, dass sie dieses Match verlieren würden und die Blockade gegen Kryptografie nicht aufrechterhalten konnten, denn die gesamte Zivilgesellschaft war dafür. So kam es schließlich zu dem folgenreichen Beschluss, rund um die Welt ab sofort Kryptografie einzuführen. Damit konnte die Kommunikation nun nicht mehr so einfach auf der Strecke abgefangen werden, sodass diejenigen, die Kommunikation abhören wollten, sich neue Wege suchen mussten – vor dem Wirken der Verschlüsselungsmechanismen – und sich somit der Integrität der Hard- und Software des Kommunikationsverursachers zuwandten.

Plattenputzer, Makroviren, Würmer

Es folgte eine Welle von Schadsoftware, und niemand wusste, wer eine so unglaubliche Menge an Personenjahren zu investieren bereit war, nur um einen Virus zu schreiben und zu verbreiten. Dass dahinter lauter *Kiddies* stecken sollten, erschien eher unglaubwürdig. Die Frage aber war, wer so etwas zu welchem Zweck, d. h. zu welchem Vorteil tun würde. Die Antwort blieb

aus, stattdessen gab es immer mehr Schadsoftware. Ende der 80er waren die meisten Prototypen von Malware bereits bekannt und ausprobiert. Ab 1995 breitete sich Malware rasant aus, insbesondere seit der massenhafteren Verwendung des World Wide Web. 1995 tauchte der erste Makrovirus für Windows Software auf. Alle computerisierten Büros waren plötzlich in Gefahr, was zu der Zeit schon beachtlich viele waren. 1998 gab es dann die erste Software der CIH-Familie, der böseste unter ihr der *Tschernobyl*-Virus, der seinem Namen alle Ehre machte. Auf infizierten Systemen löschte er komplett Festplatte und BIOS.

Während es zunächst vor allem Viren im klassischen Sinne der Medizin gab, also Programme, die echten Schaden verursachen, kamen bald auch die ersten Würmer auf – Software, die sich selbst auf eine Weise verbreiten konnte, die es bei Viren nicht gegeben hatte. Das österreichische Technikmagazin *Futurezone*, bei dem Möchel Redakteur war, berichtete zur Jahrtausendwende über viele solcher Programme, von denen ebenfalls völlig unklar war, wer die beteiligten Programmierer bezahlt hatte. Viele hatten sicherlich auf eigene Faust gehandelt oder sich kaufen lassen. Doch für dieses Geschäftsmodell erschienen die Wellen von Schadsoftware zu massiv. Die Würmer *Melissa* und *ILOVEYOU* hatten keine nennenswert böse Payload, aber verbreiteten sich so rasch, dass sie die Internet-Exchanges lahmlegten. Sie funktionierten zum Teil nach dem Schema „Nimm alle Outlook-Adressen des angegriffenen Rechners und versende dich selbst". Das Phänomen artete dermaßen aus, dass um das Jahr 2000 teilweise im Wochenrhythmus die Internetknoten für Stunden ausfielen. Es ist sehr unwahrscheinlich, dass diese Angriffe nicht koordiniert geführt wurden; plausibler ist die Erklärung, dass die Angriffe einer bestimmten militärischen Regie folgten. Abwechselnd sind die Würmer um verschiedene Internetknoten herum zuerst aufgetaucht und erst später (abgeschwächt) anderswo, etwa zuerst in Hongkong, und wenn sie später am Tag nach Europa kamen oder noch später in die USA, dann waren sie bereits verhältnismäßig harmlos. Andere Angriffe sind wiederum zuerst in den USA an der Ostküste aufgeschlagen. Deutlich wird daran, dass dabei offenbar vor allem zwei Parteien im Spiel waren. Wären diese Beobachtungen damals öffentlich gemacht worden, wären sie als paranoid weggeschoben worden, zurückgeführt hat man die Angriffe auf „irgendwelche Gangster", deren Intentionen wir eben nicht kennen. Erklären konnte man diese offensichtlichen Zusammenhänge der einzelnen Ereignisse mit dieser Theorie jedoch nicht.

Zeitgleich ist das *ECHELON*-System aufgeflogen, zu dessen Aufklärung eine Untersuchungskommission im EU-Parlament eingesetzt wurde. Möchel selbst war geladen worden, um im Gremium auszusagen. Auch die Cybercrime-Konvention fand damals statt, weil diejenigen, die *Cyber* gemacht haben, inzwischen eingesehen hatten, dass ein Regelwerk geschaffen werden musste, um nicht in einem Chaos zu enden, in dem keiner mehr weiß, was der andere tut. Daraufhin wurden die Restriktionen für Kryptografie aus dem *Wassenaar Arrangement* herausgenommen; Banken, E-Commerce und die Internetwirtschaft forderten eine zumindest so sichere Verschlüsselung, wie sie die USA hatten, mindestens Triple DES (3DES) mit 128 Bit, was für die damalige Zeit schon recht akzeptabel war. Die NSA hatte ursprünglich auf einer 40-Bit-Verschlüsselung beharrt, die jedoch mit der entsprechenden Hardware schon damals in einer Tausendstelsekunde zu knacken war. Es wurden der Wirtschaft und den Banken schließlich 56 Bit zugestanden, während auf den Heimmaschinen der Community bereits eine 128-Bit-Verschlüsselung lief und die nötige Software im Internet zum Download verfügbar war. Die Beschränkungen waren also eher lächerlich und die gesellschaftlichen Ansprüche und wirtschaftlichen Begehrlichkeiten nach Kryptografie wiederum so hoch, dass die Militärs auf verlorenem Posten standen.

Das goldene Zeitalter nach 2000

Nach 2000 explodierte das Spam-Aufkommen, woran in erster Linie die Würmer beteiligt waren. Inzwischen war eine erste Infrastruktur mit Gegenmaßnahmen entstanden: In Österreich

Erich Möchel

wurden 1999 die ersten Gesetze gegen unerlaubte Massenmails verabschiedet; in ganz Europa gab es ähnliche Bestrebungen. Beliebige Mailadressen zu sammeln und diese auf Spam-Listen zu setzen, so wie es Firmen in den 90er-Jahren regelmäßig taten, wurde ab sofort untersagt. In verschiedensten Staaten begann sich so jedoch eine Schwarzmarktindustrie zu entwickeln, und man musste sich wiederum wundern, warum dagegen nicht eingegriffen wurde. Sowohl die russischen als auch die US-amerikanischen Geheimdienste haben diese Strukturen nicht nur geduldet, statt gegen sie vorzugehen, sondern sie auch selbst benutzt – innerhalb ihrer eigenen Logiken auch rechtmäßig.

2001 drang die NSA durch Exploits in verschiedenste Firewalls aller möglichen Netze ein – erst 2016 wurde diese Verantwortlichkeit im Übrigen durch die Shadow-Brokers-Leaks bekannt. Der *Dual Elliptic Curve Random Generator* der NSA (ein kryptografisch sicherer Zufallszahlengenerator) wurde NIST-Standard und fand als solcher Verbreitung im Mobilbereich. Schon kurz nach seiner Veröffentlichung 2007 stellte sich jedoch heraus, dass sein Pseudozufall doch leichter zu rekonstruieren war als gedacht und somit ein darauf basierendes Kryptografiesystem leicht zu brechen.

Ab 2005 bildete sich der Schwarzmarkt für Botnet-Schadsoftware als Infrastruktur für Spam, Betrug, Erpressung und andere Verbrechen. Diese zivilen Kriminalitätsstrukturen eignen sich jedoch auch als Nebelwerfer für Cyber-Aktivitäten der Militärs. Ein Schwarzmarkt für Zero-Day-Exploits (bis dato geheim gehaltene Sicherheitslücken) kam in Anfängen gegen 2006 auf. Mit ihnen kam für die Kriminalitätsverfolgung eine nötige Vorsicht ins

Spiel, denn die Verfolger mussten darauf aufpassen, dass sie bei ihren Ermittlungen nicht zufällig den Partner des eigenen Militärs erwischten und vor Gericht stellten. Z. B. wurde der Autor des *Melissa*-Wurms verhaftet und war davon vollkommen überrascht – es stellte sich heraus, dass das FBI einen eigenen Mitarbeiter verhaftet hatte, der zugleich im Auftrag anderer staatlicher Organisationen arbeitete.

Ein Sprung von den 2000ern zu Snowden nach 2010

2012 veröffentlichte die Nato eine neue Cyberwar-Doktrin, weil sich Angriffe nun immer stärker häuften. Es wurde öffentlich bekanntgegeben, dass im Ernstfall „zurückgecybert wird". Doch dies ist leichter gesagt als getan, denn um einen „Gegenschlag" auszuführen, muss erst identifiziert werden, wer der Verursacher ist. Die Verschleierung ist jedoch integraler Bestandteil einer Aktion, und es dauert lange, bis ein Angriff halbwegs genau zugeordnet werden kann. Die große Gefahr besteht also insbesondere auch darin, dass *Cyber* als eine Provokation einer dritten Seite zwei Mächte gegeneinander ausspielt und gegeneinander aufbringt.

2013 enttarnte die NSA öffentlich eine Einheit der chinesischen Armee, was zu einem offenen Schlagabtausch führte. Kurz darauf ereignete sich die Veröffentlichung der Snowden-Dokumente; eine der wichtigsten Folien darunter ist der Hinweis auf 50.000 bereitgehaltene Einnistungen in Großnetze von Providern und Staat. Andere weisen auf die Quantum-Projekte hin, welche eine Zwischenschaltung in Übertragungen zu z. B. Facebook ermöglichen. Auch werden Angriffe durch Zero-Day-Exploits etwa auf den Provider Belgacom dokumentiert.

Der Cyberwar eskalierte im Ukraine-Krieg 2014: Durch ihre Steuerungssysteme wurden die örtlichen Stromnetze angegriffen. Auch der NATO-Gipfel blieb nicht verschont: Seine organisatorischen Strukturen wurden angegriffen mit der Softwaresuite *Black Energy*, eine der gebräuchlichsten Steuersoftwares zum Spammen, die allerdings zu einem Überwachungstrojaner umgebaut worden war. Zum Ziel von Sabotage und Datenklau wird immer mehr auch die Privatindustrie, besonders *Sony*, die *OPM* (eine unabhängige US-Behörde zur Verwaltung öffentlich Angestellter) oder Kranken- und Pensionsversicherungen. Der Verkauf der Daten an Kriminelle dient schlicht der Schadensmaximierung. All dies waren die ersten Cyber-Auseinandersetzungen, die wir im Grunde live mitverfolgen konnten.

Das *Wassenaar Office* soll nun dafür sorgen, dass Schadprogramme aus der NATO nicht in falsche Hände geraten – es ist freilich aber schlicht und einfach festzustellen, dass jegliche Hände dafür falsch sind. Da das Wassenaar-Abkommen aber auch noch weitere Staaten einbezieht, wie z. B. Russland oder die Ukraine, schlägt sich zudem deren politischer Konflikt auf die Sitzungen nieder. Nach dem arabischen Frühling kam auf EU-Initiative die Kontrolle sogenannter Cyber-Waffen als neuer Punkt für das Abkommen hinzu, denn vor allem europäische Firmen liefern Überwachungssoftware an die Regime. Problematisch an der Arbeit des Office: Es gibt keine Öffentlichkeitsarbeit. Der Artikel über die Regulierungslisten 1998 in Telepolis von Möchel war der erste Bericht zum Thema überhaupt.

Schlussfolgerungen

Der Cyberwar ist kein herkömmlicher Krieg, sondern folgt anderen Regeln, die 6000 Jahre Militärgeschichte auf den Kopf stellen. Wo die Verteidiger bisher stets bei allen Strategien im Vorteil waren, ist es im Cyberbereich der Angreifer. Er wählt den Zeitpunkt, den Ort des Angriffes im Netz und die Angriffsweise. Allein schon durch die schiere Menge der Angriffsvektoren ergibt sich ein enormer Nachteil in der Verteidigung. Als Konsequenz ergeben sich mehr mögliche und schnell erreichbare Angriffsziele, je besser ein Land vernetzt ist und je dichter seine Infrastruktur ausgebaut ist. In weniger computerisierten und international vernetzen Ländern sind Cyber-Angriffe wesentlich weniger leicht durchzuführen. Für den Staat ist Angriff also billig und lässt sich sogar an halbstaatliche/kriminelle Gruppen auslagern; Verteidigung dagegen ist extrem teuer. Probleme ergeben sich aber durchaus auch innerstaatlich, wenn solche Gruppen wie in Russland z. B. ungeplant über ihren Auftrag hinaus auf Fang bei russischen Banken gehen. Sicherheit, Crypto und Cyber gehören somit zusammen als Verteidigungs- und Angriffstechnologien.

Wie sich unsere Cyber-Zukunft weiterentwickeln wird, das steht mehr als anderes in den Sternen, weil Cyber-Angriffe derzeit noch mitunter sehr konfus und anarchistisch ablaufen. Fest steht: Computer sind nach den Angriffen immer noch da und können mit Backups wieder gangfähig gemacht werden, werden auch selbst immer robuster. Aber es gibt im Cyberkrieg keine Verlierer und Gewinner. Nur temporäre Erfolge, und darum ist das, was alle unter *Cyber* verstehen, nicht nur eine (Kriegs-)Politik mit anderen Mitteln, sondern mehr noch die Fortsetzung der Diplomatie mit anderen Mitteln. Denn dann, wenn Diplomat.innen aufhören zu reden, beginnen Gesten, Militärmanöver und Flottenparaden. Noch haben Cyber-Operationen als Provokation keine konventionellen Gefechte ausgelöst, auch weil bisher vorsichtig damit umgegangen wurde. Trotz der Gefahr dieser Angriffe ist es zwar sehr unwahrscheinlich, dass Cyberwaffen konventionelle Waffen ablösen werden; nach mehr als zwanzig Jahren derartiger Computersabotage und -lücken bleibt es jedoch nun uns überlassen, einen Ausweg aus dem Cyberwar zu finden.

Erich Möchel

Erich Möchel ist seit 1983 Medienkritiker und Kulturjournalist; für den *Falter*, das Radio OE1, den Standard, das Wirtschaftsblatt, für heise.de, quintessenz, Futurezone, den ORF und einige mehr. Er beschäftigte sich schon lange vor Edward Snowden und Echelon kritisch mit geheimdienstlichen Abhörpraktiken. Darüber hinaus ist er Mitglied beim Österreichischen Journalisten-Club und im International Board of Advisors von Privacy International. Er ist zudem Autor mehrerer Romane und Theaterstücke.