BERLINER KOLLEG
KALTER KRIEG
BERLIN CENTER
FOR COLD WAR STUDIES

Kalter Krieg und Cybersecurity

Klaas Voss /
Universität Den Haag

Ein Schlüsselkonzept der modernen Militärwissenschaft sind die so genannten fünf "Domänen der Kriegführung". Sie beschreiben einen einfachen Sachverhalt: Technologische Überlegenheit kann in militärische Überlegenheit umgemünzt werden, indem sie zur Kontrolle über neue Arten von militärischen Räumen ("Domänen") genutzt wird. Land, Meer, Luft, Weltraum – jeder dieser Räume erlebte seine militärische Pionierzeit und wurde mit U-Booten und Streitwagen, mit Chronometern und GPS-Satelliten dominiert. Der Kalte Krieg wird natürlich zu Recht mit der amerikanisch-sowjetischen Rivalität im Weltraum assoziiert, die gleichbedeutend mit dem Wettlauf um die besten Trägersysteme für Kernwaffen und die leistungsfähigsten Aufklärungs- und Navigationssatelliten war. Doch es gab noch einen weiteren militärischen Raum, der insbesondere im letzten Jahrzehnt des Kalten Krieges sondiert und erschlossen wurde. Ein US-Luftwaffengeneral taufte ihn 1995 die "Fifth Dimension of Warfare", gemeint war die virtuelle Welt der Information. In der Populärkultur setzte sich schon früher, in den 1980er Jahren, ein anderer Begriff durch: der vom kybernetischen Raum, dem "Cyberspace".

Die Schnittstellenwissenschaft der Kybernetik, die alle Bereiche der Gesellschaft miteinander verschalten, plan- und steuerbar machen

wollte, war nicht weniger ein Projekt des Kalten Krieges als die Spieltheorie, das mathematische Betriebssystem des Nuklearkrieges. Bemerkenswert ist übrigens auch – und gerade – die gesellschaftliche Bedeutung der Kybernetik und der frühen Computerwissenschaften in der Sowjetunion, die Slawa Gerowitsch in seine Forschungen nachzeichnete. Während der sowjetische Verwaltungsapparat noch von der perfekten "Kyberbürokratie" träumte, entwickelte die amerikanische Advanced Research Project Agency (ARPA) 1969 bereits das technische Grundmodell des späteren Internets – das Arpanet. Es ist zwar ein Mythos, dass dieses Projekt ausschließlich militärische Hintergründe hatte und einer Aufrechterhaltung der landesweiten Kommunikation im Falle eines Nuklearschlages diente, doch ebenso wenig ist die Geschichte des Internets vom Kalten Krieg und der Bedrohung durch Nuklearwaffen zu trennen. Die RAND Corporation verfasste bereits 1960 eine Studie über den Einsatz von digitalen Datenfernübertragungsnetzwerken zugunsten eines schnellen nationalen Wiederaufbaus nach einem Atomschlag. Diese Zitate sind zu bizarr, um sie zu paraphrasieren:

"The cloud-of doom attitude that nuclear war spells the end of the earth is slowly lifting from the minds of many. Better quantitative estimates of post-attack destruction together with a less emotional discussion may mark the end of the 'what the hell – what's the use' era. [...] If war does not mean the end of the earth in a black and white manner, then it follows that we should do those things that make the shade of grey as light as possible: to plan now to minimize potential destruction and to do

all those things necessary to permit the survivors of the holocaust to shuck their ashes and reconstruct the economy swiftly." (Zur Quelle)

Inwiefern das spätere Internet wirklich geholfen hätte, die "Asche des Nuklearkrieges abzustreifen", bleibt sicherlich Spekulation. Doch bereits unter den Präsidenten Carter und Reagan produzierten die NSA und das Militär Strategiepapiere zur Sicherheit digitaler Kommunikationswege und Datenbestände. Es war die Geburtsstunde der Cybersecurity, die in den Folgejahren zu einer neuen "Frontier" der Nationalen Sicherheit werden sollte – und es bis heute bleibt.

Das National Security Archive an der George Washington University in Washington, DC, hat es sich in einem neuen Projekt zur Aufgabe gemacht, durch Anfragen unter dem Freedom of Information Act (FOIA) Licht in diesen bisher kaum erforschten Bereich US-amerikanischer Sicherheitspolitik zu bringen und bisher gesperrte Dokumente zu allen Arten von "cyber issues" aus staatlichen und privaten Beständen für Forscher und eine interessierte Öffentlichkeit zugänglich zu machen. Das Cyber Vault Project verfügt derzeit über eine Volltextdatenbank mit 388 Dokumenten aus dem Zeitraum von 1964 bis 2016. Dies mag auf den ersten Blick überschaubar klingen, doch wer mit der bisherigen Arbeit des National Security Archive vertraut ist, mag ahnen, dass es nicht bei dieser Zahl bleiben wird. Das Archiv verfügt über 45 vollständig digitalisierte Quellensammlungen mit insgesamt über 104.000 Dokumenten, viele davon aus dem geheimdienstlichen, militärischen oder präsidialen Bereich und mit (ursprünglich) hohen Sicherheitseinstufungen. Die Arbeit mit den Quellenbeständen der

Institution kommt für viele Historiker des Kalten Krieges, die sich mit entsprechend sensiblen außen- und sicherheitspolitischen Bereichen der US-Politik befassen, einem Initiationsritus gleich. So bleibt auch beim Cyber Vault Project trotz der aufwändigen FOIA-Anträge auf eine schnelle Vergrößerung zu hoffen. Seit einem ersten Blick in die Datenbank des Cyber Vault Project vor wenigen Wochen sind die Bestände bereits um rund 25% gewachsen.

Dr. Jeffrey T. Richelson ist ein Senior Fellow am National Security Archive und verantwortlich für das Cyber Vault Project. Eine Vielzahl seiner Publikationen beschäftigt sich mit den Schnittpunkten zwischen militärisch-sicherheitspolitischen und technologisch-wissenschaftlichen Themen. In einer E-Mail beschreibt Richelson das Ziel des neuen Projekts:

"It was apparent that while there was a vast literature on cyber issues, references to documents, and occasional postings of documents, there was no collection of such documents that came close to being comprehensive. It seemed clear that such a collection would be interesting and useful to both those researching contemporary cyber activities (whether cybersecurity, cyber espionage, or cyber war) as well as looking back into earlier years. The objective is to establish a major repository for such documents that would allow researchers to find both individual documents relevant to their work but also sets of documents that would facilitate their research."

Richelson merkte zwar auch an, dass der Zusammenhang zwischen dem Kalten Krieg und Fragen der Cybersecurity nicht im Zentrum des Projekts stünden, doch dies mindert keineswegs die Nutzbarkeit der publizierten Dokumente für Forschungen in diese Richtungen. So warnt beispielsweise ein vom Cyber Vault Project zugänglich gemachtes RAND-Papier von 1967 vor ausländischen bzw. sowjetischen Spionageattacken auf Computernetzwerke des US-Militärs: "Computer systems are now widely used in military and defence installations and deliberate attempts to penetrate [them] must be anticipated".

Dass Computersysteme vor Spionen geschützt werden müssen, mag 1967 eine innovative Erkenntnis gewesen sein. Aus gegenwärtiger Sicht kurios muten hingegen die im RAND-Papier diskutierten Verwundbarkeiten an: Wo heute Computerexperten Rootkits, DoS-Attacken und Bot-Netze fürchten, warnten die Ingenieure von 1967 vor Sicherheitslücken durch den Austausch des Monitors (der freilich zu dieser Zeit ein integraler Bestandteil des Systems war) oder dem "Belauschen" der elektromagnetischen Wellen von Prozessoren und Kabeln. Die Begriffe "Virus" oder "Trojaner" waren noch nicht verbreitet, stattdessen wurde der heute für Programmfehler genutzte Terminus "Bug" verwendet. Ein solcher von Spionen platzierter "Bug" sei "some computer equivalent of the famous transmitter in a Martini olive".

Doch auch den Computeringenieuren von 1967 war klar, dass die größte Sicherheitslücke immer noch beim User zu sehen war (IT-Experten haben sich zumindest in dieser Hinsicht nicht wesentlich verändert). Das mögliche Abhören der elektromagnetischen Emissionen von Kabeln und

Prozessoren durch Spione verursachte bis in die 1970er Jahre große Besorgnis, wie ein freigegebener Bericht der US Defense Science Board Task Force for Computer Security zeigt. Die Methode mag eher an Morsecode im Telegrafenzeitalter erinnern, doch man sollte vorsichtig mit vorschneller Belustigung über die Zeitgenossen sein: Bis heute wird ein Großteil des Netzwerkverkehrs über Kupfer- und nicht über Glasfaserkabel übertragen und wäre somit (zumindest in der Theorie) für solche Angriffe verwundbar.

In den 1970er und 1980er Jahren wurde das entstehende Wissenschaftsfeld der Cybersecurity zunehmend zur Frage der Nationalen Sicherheit und beschäftigte Geheimdienste, das Pentagon und das Weiße Haus. "Cryptolog", die Hauszeitschrift der NSA, widmete mehrere Ausgaben der Diskussion neuer Sicherheitskonzepte. Eines der vom National Security Archive zugänglich gemachten Hefte aus dem Jahr 1979 erwähnt (als zukünftige Forschungsfelder) fast beiläufig eine ganze Reihe von solchen Schlüsselelementen moderner Computersicherheit.

Das bisher vielleicht interessanteste Dokument aus der Zeit des Kalten Krieges ist jedoch Präsident Ronald Reagans National Security Decision Directive Nr. 145 vom 17. September 1984. Hierin erklärte Reagan den Schutz von "Automated Information Systems" buchstäblich zur Chefsache. Dieser sei mittlerweile ein "vital element of the operational effectiveness of the national security activities of the government and of military combat readiness" geworden. Das World Wide Web – für die meisten Menschen gleichbedeutend mit dem Internet – existierte zu diesem Zeitpunkt noch nicht einmal, doch die informationstechnische

Vernetzung von Militär- und Regierungsinstitutionen hatte den wachsenden Cyberspace bereits zu einem neuen Grenzland der Nationalen Sicherheit gemacht. Reagans Besorgnis beschränkte sich zu diesem Zeitpunkt nicht mehr allein auf die Sowjetunion und fremde Nationen. Die zukünftigen Bedrohungen der Computersicherheit, so steht es in NSDD 145, mochten ebenso von Terroristen oder Kriminellen ausgehen. Es war eine weitsichtige Erkenntnis.

Dr. Klaas Voß ist Dozent an der Universität Den Haag (The Hague University of Applied Sciences) im Studiengang "Safety and Security Management Studies".

Zitierempfehlung:

Klaas Voss, Kalter Krieg und Cybersecurity, 30.08.2016, http://www.berlinerkolleg.com/de/blog/kalter-krieg-und-cybersecurity (bitte fügen Sie in Klammern das Datum des letzten Aufrufs dieser Seite hinzu).