

Computergestützte Frühwarn- und Entscheidungssysteme

K. H. Bläsius und J. H. Siekmann

Universität Kaiserslautern

Zusammenfassung. Die massive Bedrohung durch Nuklearwaffen, die den Supermächten die Möglichkeit zur Auslöschung allen Lebens auf der Erde geben, erfordert eine Entscheidungsfindung oftmals innerhalb weniger Minuten. Dies hat beide Seiten zum Aufbau von Frühwarn- und Entscheidungssystemen (FWES) veranlaßt, durch deren Einsatz ein atomarer Angriff noch innerhalb der Raketenflugzeit erkannt werden soll. In diesem FWES spielt die Verarbeitung und Weiterleitung von Informationen durch den Computer eine kriegsentscheidende Rolle: Die Informatik ist zu einer der wichtigsten Grundlagenwissenschaften in der Rüstungsforschung geworden. Dieser Artikel gibt eine Übersicht über die Funktionsweise computergestützter FWES und zeigt Fehlerquellen auf, die es möglich und sogar wahrscheinlich machen, daß eine Verkettung unglücklicher Umstände zu einem Nuklearkrieg „aus Versehen“ führen kann.

Schlüsselwörter: Nuklearkrieg, Frühwarnsysteme

Summary. This article surveys function and structure of computer-based early-warning systems. Potential malfunction is analyzed, with the conclusion that unfavorable conditions can lead to chain reactions by both superpowers that may cause an accidental nuclear war.

Key words: Nuclear war, Early-warning systems

1. Einleitung

Seit Ende des zweiten Weltkrieges haben die beiden Supermächte UdSSR und USA Nuklearwaffen auf immer schnelleren Trägern, von der strategischen Bomberflotte nach dem 2. Weltkrieg bis zu den heutigen Interkontinentalraketen oder U-Bootraketen, entwickelt. Während die Flugzeiten der Interkontinentalraketen etwa 30 Minuten betragen, sind die an den amerikanischen Küsten operierenden Yankee-U-Boote der UdSSR in der Lage, innerhalb weniger Minuten die amerikanischen Kommandozentralen auszuschalten oder durch die gezielte Auslösung eines EMP (elektromagnetischer Impuls, der eine in größerer Höhe gezündete Atom-

bombe begleitet) den für den Gegenschlag notwendigen Nachrichtenverkehr zu behindern [5]. Ebenso können die USA die Kommandozentralen und Abschußsilos der UdSSR durch die neuen Mittelstreckenraketen Pershing-II innerhalb weniger Minuten erreichen [3].

Diese massive beiderseitige Bedrohung, die eine Entscheidungsfindung oftmals *innerhalb weniger Minuten* erfordert, hat beide Seiten zum Aufbau von Frühwarn- und Entscheidungssystemen (FWES) veranlaßt, durch deren Einsatz ein atomarer Raketenangriff des Gegners noch innerhalb der Raketenflugzeit erkannt werden soll. Damit kann die eigene Reaktion frühzeitig geplant und unter Umständen auch noch während der Flugzeit ausgeführt werden, bevor die gegnerischen Raketen mit ihrer vernichtenden Wirkung ein Zurückschlagen erschweren oder verhindern.

Die gesamte Früherkennung und Entscheidungsfindung ist wegen der enorm kurzen Zeitspannen zwischen Start und Einschlag und der Komplexität der zu bewertenden Informationen auf das zuverlässige Arbeiten von Computern abgestellt: Das „World Wide Military Command and Control System (WWMCCS)“ der USA und die westlichen Kommandozentralen gehören zu den komplexesten technischen und organisatorischen Systemen, die je von Menschen erbaut wurden [5].

Bei einer Alarmmeldung wird die Entscheidung für eine angemessene Reaktion von den auf verschiedenen Ebenen in dieses System integrierten Menschen getragen. Die Zeit, die den Menschen zur Verfügung bleibt, um solche Entscheidungen zu treffen oder die Alarmmeldung als Computerfehler zu erkennen, ist jedoch in besonderen Situationen so kurz, daß eine Überprüfung der technischen Daten kaum möglich ist.

Wie ein sowjetischer nuklearer Angriff auf die USA aus der Sicht der Raketenwarnsysteme ablaufen könnte, beschreiben die beiden Senatoren Gary Hart und Barry Goldwater in einem Untersuchungsbericht für den amerikanischen Senat ([22], S. 3):

„Sollte die UdSSR U-Boot-gestützte und Interkontinentalraketen getrennt oder gleichzeitig starten, würde mit sehr großer Wahrscheinlichkeit folgendes passieren:

Die erste Anzeige eines Raketenstarts kommt von den Satelliten, gefolgt von der Feststellung des Starts U-Boot-gestützter Raketen durch die Radarstationen

PAVE PAWS. Einige Minuten später stellt das BMEWS (Ballistic Missile Early Warning System) den Start von Interkontinentalraketen fest. Die Satelliten melden den Start sowohl von SLBMs (Submarine Launched Ballistic Missiles) als auch von ICBMs (Intercontinental Ballistic Missiles), kurz nachdem dieser erfolgt ist. Die Radarstationen PAVE PAWS registrieren die SLBMs innerhalb weniger Minuten nach dem Start. Einige Minuten später stellt das BMEWS die Interkontinentalraketen fest. Das PARCS (Perimeter Acquisition Radar Attack Characterization System) registriert die Interkontinentalraketen in der Schlußphase des Fluges.

Der Zeitraum vom Start bis zum Auftreffen von U-Boot-gestützten Raketen könnte wesentlich kürzer als bei Interkontinentalraketen sein, bei denen er ca. 30 Minuten beträgt. Da die SLBMs einen Großteil der Bodensensoren und Kommandostellen zerstören könnten, muß davon ausgegangen werden, daß die Zeitspanne von der Feststellung eines Raketenstarts bis zum Auftreffen der ersten Rakete – in dieser Zeit kann das gegenwärtige System voll genutzt werden – kurz sein kann. Das bedeutet nicht, daß das gesamte System danach nicht mehr besteht, aber es bedeutet, daß wir abhängig werden von solchen Teilen des Systems, die den Eröffnungsangriff überstehen, d.h. allgemein von solchen, die sich rechtzeitig in der Luft befinden, um dem Angriff zu entgehen. Deshalb ist die volle und effektive Nutzung des kurzen Zeitraums zwischen der Feststellung eines Raketenangriffs und der Zerstörung des größten Teils der Infrastruktur (Kommandostellen und Steuerung) außerordentlich wichtig.“

Zur Bewertung von Alarmmeldungen stehen der Kontrollmannschaft und dem Präsidenten, der bei der höchsten Alarmstufe mit einbezogen wird, nur wenige Minuten zur Verfügung. Diese Zeit kann beispielsweise mitten in der Nacht liegen und die politischen Führungspersonen in einer schwierigen Verfassung, z.B. nach einem äußerst anstrengenden Tag oder nach Kompetenzproblemen [2], treffen. Unter den enormen psychischen Belastungen, die diese Vorbedingungen und die mögliche Tragweite einer Entscheidung für die Kontrollmannschaft und den Präsidenten bewirken, dürfte es schwierig sein, eine korrekte Bewertung und angemessenes Handeln zu gewährleisten.

In allen technischen Bereichen geschehen Unfälle durch technisches Versagen, menschliches Fehlverhalten oder eine Kombination dieser beiden Fehlerquellen. Es stellt sich daher die Frage, wie zuverlässig sind die hochkomplexen Frühwarn- und Entscheidungssysteme (FWES) unter den bestehenden extremen Zeitrestriktionen? Können computergestützte FWES durch menschliches oder technisches Versagen, insbesondere durch Computerfehler, einen Atomkrieg aus Versehen auslösen? Wenn ja: Unter welchen Umständen ist ein solcher Unfall möglich?

Die Sicherheitsmaßnahmen gegen einen solchen Unfall lassen sich in drei große Bereiche einteilen [28]:

- technische und organisatorische Sicherungssysteme,
- multilaterale politische und vertragliche Sicherheitsmaßnahmen,
- militärstrategische Maßnahmen.

Die technischen Sicherungssysteme sollen verhindern, daß beispielsweise ein U-Boot-Kommandant, der die Nerven verliert, einen Krieg auslösen kann. Daher kann eine Atomrakete nur mit mindestens zwei Schlüsseln (bzw. entsprechendem Computercode), die von verschiedenen Personen getragen werden, gefechtsbereit gemacht und gestartet werden. Ebenso wurden aufwendige technische Sicherungssysteme eingebaut, die verhindern sollen, daß eine Rakete von allein oder versehentlich starten kann.

Zu den organisatorischen Sicherungssystemen zählen die Überwachung und Kontrolle der die Entscheidung treffenden Menschen ebenso wie eine hohe Redundanz in der Informationsverarbeitung, um auch beim Ausfall eines technischen Gerätes, einer Übertragungsleitung oder einer Kommandoeinheit die Funktionsfähigkeit zu erhalten.

Der zweite Bereich betrifft die vertraglichen Vereinbarungen, beispielsweise die Einrichtung des „Heißen Drahtes“ und die vertragliche Verpflichtung, daß im Falle eines Alarms über den „Heißen Draht“ eine Kommunikation zwischen dem Präsidenten der Vereinigten Staaten und dem Generalsekretär der KPdSU möglich ist.

Der dritte wichtige Bereich ist der strategische. Bisher haben sich beide Seiten auf eine Militärstrategie geeinigt, in der höchstens dann mit Nuklearwaffen zurückgeschossen wird, wenn zweifelsfrei feststeht, daß mindestens eine Atomrakete auf dem eigenen Territorium eingeschlagen ist. „Launch on Impact“ wird diese Strategie genannt, die weitgehend sichergestellt hat, daß trotz zahlreicher bisheriger Fehlalarme der Computersysteme kein „Weltkrieg aus Versehen“ ausgelöst wurde. Diese Strategie war wegen der gesicherten „Zweitschlagfähigkeit“ möglich, d.h. trotz eines unglaublichen Zerstörungen anrichtenden Erstschlages war jede Seite zum vernichtenden Gegenschlag in der Lage: „Wer zuerst schießt, stirbt als zweiter“.

Die gegenwärtige militärtechnologische Situation ist, zusammenfassend gesagt, durch zwei Faktoren geprägt:

- Zum ersten Mal in der menschlichen Geschichte sind wir technisch in der Lage, nicht nur ganze Landstriche oder Städte zu verwüsten, sondern das menschliche Leben auf diesem Planeten als ganzes auszulöschen.
- Die Entscheidungsfindung für den Einsatz dieser fürchterlichen Waffen muß in immer kürzeren Zeitspannen erfolgen: Während dem Generalstab im letzten Weltkrieg beispielsweise für wichtige militärische Entscheidungen fast immer ein oder zwei Tage zur Verfügung standen (er die Entscheidung also noch einmal „eine Nacht überschlafen konnte“), wurde diese Zeitspanne immer rascher reduziert. Nach dem zweiten Weltkrieg lag die maximale Zeitspanne zur Entschei-

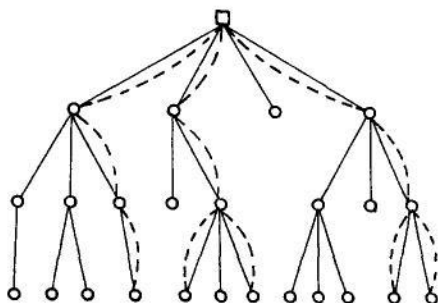
dungsfindung im Stundenbereich (strategische Bomberflotten), danach im Minutenbereich (Interkontinentalraketen, ca. 30 Min.) und wurde jetzt durch die Mittelstreckenraketen auf ca. fünf bis acht Minuten reduziert. Falls sich das SDI-Programm verwirklichen läßt, wird diese Zeitspanne in den Sekundenbereich sinken.

Welche militärischen Kommandostrukturen sind einer solchen Situation angemessen? Wie sehen diese Strukturen aus der Sicht eines Informatikers aus; wie wird darin Information verarbeitet und weitergeleitet?

2. Militärische Kommandostrukturen im Nuklearzeitalter

Die klassische Armeeführung basiert auf einer streng hierarchisch gegliederten Kommandostruktur, die im wesentlichen identisch mit dem Informationsfluß zwischen den einzelnen Einheiten ist. Diese über Jahrhunderte entwickelte Struktur wurde zwar in Einzelheiten geändert und der fortschreitenden Waffentechnologie angepaßt, der hierarchische Grundaufbau jedoch nicht in Frage gestellt. Auch in den beiden vergangenen Weltkriegen wurde die Kriegführung nach diesem Prinzip abgewickelt: An der Spitze stand die politische und militärische oberste Armeeführung, die globale Einsatzbefehle an die niedrigeren Organe weitergab, die dann von diesen im wesentlichen selbständig ausgeführt oder an die jeweiligen Untereinheiten weitergegeben wurden. Auftretende Probleme wurden in der Regel nicht an die Spitze der Hierarchie gesendet, sondern so weit unten wie möglich in der Hierarchie gelöst. Dort konnte man sich dann auf das lokale Problem konzentrieren, ohne das ganze Umfeld berücksichtigen zu müssen. Die Komplexität der Informationsverarbeitung, die eine einzelne Kommandozentrale weit überfordert hätte, wurde also durch die hierarchische Struktur bewältigt ([5], S. 57).

Abbildung 1 soll diese klassische Kommandostruktur, in der die *Ranghierarchie* mit dem *Informationsfluß* weitgehend identisch war, verdeutlichen.



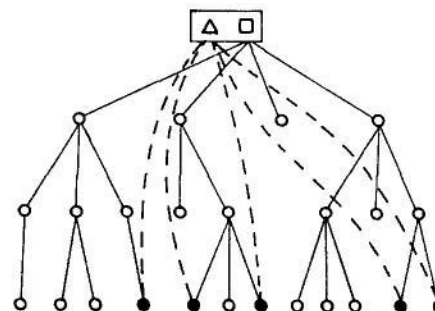
- oberste Armeeführung
- militärische Organe
- Ranghierarchie
- Informationsfluß (Einsatzbefehle etc.)

Eine solche Kommandostruktur hat entscheidende Vorteile: Obwohl die Spitze der Hierarchie alle wesentlichen globalen Entscheidungen wie Angriff oder Verteidigung, Vormarsch oder Rückzug beeinflussen kann, ist sie nicht durch die Komplexität der Informationsverarbeitung, die eine direkte Kontrolle aller Einheiten und aller Operationen bedeuten würde, überfordert. Insbesondere bleibt diese Kommandostruktur auch dann noch stabil, wenn große Teile des Systems ausfallen, jedenfalls solange die Spitze dieser Hierarchie funktionsfähig bleibt.

Der Aufbau der Nuklearstreitkräfte seit dem zweiten Weltkrieg schaffte jedoch Bedingungen, denen die hierarchische Kommandostruktur nicht mehr gerecht wurde.

Unter dem Eindruck der katastrophalen Verwüstungen, die die Atombomben auf Hiroshima und Nagasaki auslösten, stand zunächst der Gesichtspunkt der zivilen Kontrolle über den Einsatz dieser Waffen im Vordergrund: Unmittelbar nach dem zweiten Weltkrieg unterstanden die amerikanischen Nuklearwaffen direkt dem Präsidenten und einem zivilen Kommando, nicht den Militärs. Ebenso waren die sowjetischen atomaren Waffen nicht direkt den Militärs unterstellt, sondern einer speziellen Einheit des KGB [5].

In Abb. 2 sind die Kommandostruktur und der zusätzliche Informationsfluß dargestellt.



- oberste Armeeführung
- △ Präsident
- militärische Organe
- militärische Organe mit Nuklearwaffen
- Ranghierarchie
- Informationsfluß (Einsatzbefehle etc.)

Neben dem normalen Informationsfluß innerhalb der Hierarchie gab es zusätzliche Informationskanäle zwischen den Einsatzkommandos für Nuklearwaffen und dem Präsidenten.

Der erfolgreiche Start des sowjetischen Sputnik am 4. Oktober 1957 löste in den USA einen Schock aus: Damit war ja nicht nur die Fähigkeit der UdSSR demonstriert, einen Nachrichtensatelliten erfolgreich zu platzieren, sondern auch, Atomsprenköpfe mit Hilfe von Raketen direkt auf das Territorium der USA zu

transportieren, ohne daß es dagegen eine Abwehrmöglichkeit gäbe. Unter diesem Eindruck begann bei den Militärs und der politischen Führung ein Umdenken: Wie kann man verhindern, daß die militärische Führung innerhalb von Minuten ausgelöscht und die gesamten Streitkräfte damit gelähmt und zum Gegenschlag unfähig werden?

Welche für die Kommandostruktur wesentlichen Randbedingungen schaffen diese Raketenträger?

(1) Die Sprengkraft und die übrigen Auswirkungen von Atomraketen sind so groß, daß es – ebenfalls im Gegensatz zu früheren Kriegen – möglich ist, die gesamte oberste Armeeführung des Gegners auf einen Schlag zu vernichten.

(2) Während die wichtigen militärischen Entscheidungen selbst in den letzten beiden Weltkriegen noch innerhalb von Tagen und nur in Ausnahmefällen innerhalb weniger Stunden getroffen werden mußten, müssen die Entscheidungsprozesse heute – einschließlich der Befehlsübermittlung – im *Minutenbereich* ablaufen: Vom Zeitpunkt des Zündens der feindlichen Raketen bis zum Eintreffen müssen die wichtigsten Gegenmaßnahmen geplant und eingeleitet sein.

Diese beiden durch die neue Waffentechnologie geschaffenen Randbedingungen erfordern neben dem Betrieb von computergestützten Raketenwarnsystemen auch neue Kommandostrukturen, da die hierarchische Struktur unter diesen neuen Restriktionen völlig unbrauchbar geworden ist:

- Die Entscheidungsprozesse kamen durch einen wiederholten Informationsfluß auf- und abwärts in der Hierarchie zustande und wären heute viel zu langsam.
- Die Zerstörung der Hierarchiespitze würde die gesamten Streitkräfte paralisieren.
- Die lokale, d. h. dezentrale Entscheidung einer kleinen militärischen Einheit, taktische oder strategische Atomwaffen einzusetzen, würde eine Eskalation des Krieges bedeuten, die so fundamentale Folgen hätte, daß man diese Entscheidung nicht dezentral, sondern nur zentral fällen kann.

Welche militärische Kommandostruktur und welcher Informationsfluß ist einer solchen Situation angemessen?

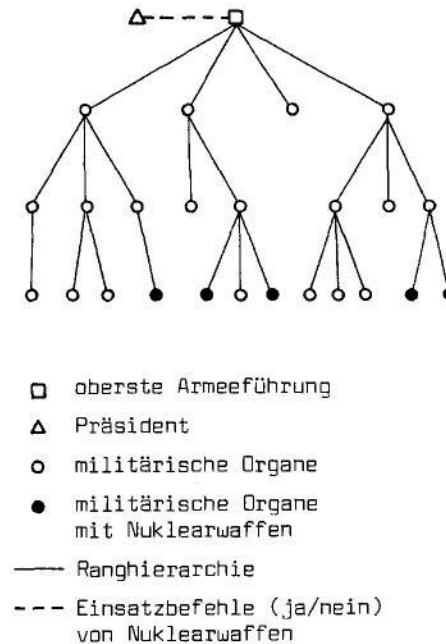
Eine zentrale (hierarchische) Struktur scheidet wegen der geschilderten hohen Verwundbarkeit aus, und eine völlig dezentralisierte Entscheidungskompetenz ist wegen der katastrophalen Folgen eines atomar geführten Krieges aus Sicherheitsgründen ebenfalls unmöglich.

Die fundamentale Umstrukturierung der Streitkräfte, als Antwort auf diese neue Herausforderung, vollzog sich im wesentlichen in drei Abschnitten [5]:

A) Die Zeit von 1955 bis 1960: Mobilmachung im Minutenbereich

In dieser Zeitspanne wurden erstens die Voraussetzungen geschaffen, um die Mobilmachung der Streitkräfte,

die einen atomaren Gegenschlag ausführen sollen, in den Minutenbereich zu bringen: Die jederzeit einsatzfähigen Bomberflotten mit der permanent anwesenden Bombercrew konnten am Ende dieser Periode innerhalb weniger Minuten aufsteigen und einen Gegenschlag ausführen. Die Rolle der obersten Führung und des Präsidenten blieb in dieser Hinsicht auf die eines „Auslösers“ (den einmaligen Einsatzbefehl) beschränkt, und das Militär bekam wesentlich mehr Einfluß auf den tatsächlichen Einsatz nuklearer Waffen (Abb. 3).



Zweitens wurden in dieser Periode die Grundlagen für die Frühwarnsysteme geschaffen: NORAD (North American Aerospace Defense Command Center) wurde in die Cheyenne Mountains verlegt, SAC (Strategic Air Command) wurde gegründet, und die Nachrichtensysteme, aus denen das BMEWS (Ballistic Missile Early Warning System) besteht, entstanden als die bis dahin größten Informationsverarbeitungssysteme, die je von Menschen gebaut worden waren. Der heutige Stand dieser Systeme wird in den folgenden Abschnitten genauer beschrieben.

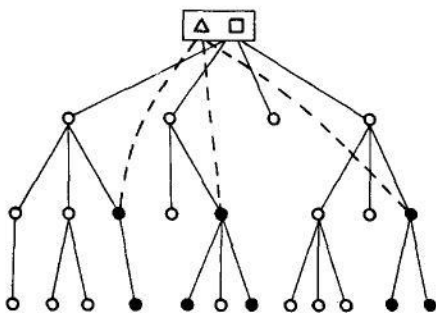
B) Die Zeit von 1961 bis 1967: Veränderungen in der Kommandostruktur

Unter dem Einfluß der Kubakrise, in der die effektive Führung dem amerikanischen Präsidenten zeitweilig entglitten war, und einer historischen Beschäftigung mit dem ersten Weltkrieg, in den die Weltmächte aus seiner Sicht durch ein gegenseitiges, systembedingtes Aufschaukeln der Spannungen „hineinglitten“, ohne es eigentlich wirklich zu wollen, initiierte Präsident Kennedy tiefgreifende Veränderungen in der Struktur der amerikanischen Streitkräfte mit dem Ziel, den zivilen Einfluß wieder zu stärken. Aus tiefer Besorgnis über die Möglichkeit eines „dritten Weltkrieges aus Versehen“

und durch die Beschäftigung mit dem ersten Weltkrieg angeregt, soll er gesagt haben:

„If this planet is ever ravaged by nuclear war – if the survivors of that devastation can endure the fire, poison, chaos and catastrophe – I do not want one of the survivors to ask another ‚How did it all happen?‘ and to receive the incredible reply, ‚Ah, if only one knew‘“ [29].

Wie kann man jedoch die politische Führung stärken, ohne sie durch die dann notwendige umfangreiche Informationsverarbeitung für die detaillierten Einsatzbefehle der einzelnen Einheiten völlig zu überlasten? Die Antwort war eine völlige Umstrukturierung der Streitkräfte (Abb. 4 zeigt die tiefgreifende Umstrukturierung [5] nur unvollkommen, wichtig ist hier die erneute Dezentralisierung und der neue Informationsfluß).



- oberste Armeeführung
- △ Präsident
- militärische Organe
- militärische Kommandoeinheiten mit Nuklearwaffen
- Ranghierarchie
- Informationsfluß bzgl. des Einsatzes von Nuklearwaffen

In dieser Struktur haben der Präsident und die politische Führung also wieder direkten Einfluß auf die einzelnen Nukleareinheiten und können beispielsweise eine beschränkte Kriegsführung, wie sie die neue Doktrin des ‚flexible response‘ verlangt, durchsetzen. Die Ausföhrung und die damit verbundene detaillierte Befehlsausgabe liegt jedoch in den einzelnen Einheiten selbst.

C) Die Zeit seit 1968: Verletzbarkeit der Kommunikationsstruktur

Die geschilderte Kommandostruktur sichert zwar wieder eine direkte politische Einflußnahme, ist jedoch nur so lange funktionsfähig, wie die Kommunikationskanäle nicht zerstört sind. Insbesondere schafft sie keine Antwort auf das eigentliche Problem: Was passiert, wenn das Zentrum der politischen und militärischen Führung ausfällt?

Die Antwort darauf war ein Plan von verblöffender Raffiniertheit, der die bisherige Vorstellung von militärischer Kommunikation und von Einsatzbefehlen auf

den Kopf stellt. Die Kommandostruktur bleibt zwar erhalten, wie in Abb. 4 graphisch dargestellt, jedoch die *Übertragung der Information* erfolgt anders: Um der Bedrohung der Vernichtung des Zentrums zu entgehen, sind die Einsatzpläne für einen massiven atomaren Gegenschlag dezentral auf möglichst viele Kommandostellen verteilt und treten automatisch in Kraft, falls die übergeordnete Kommandozentrale oder gar das Pentagon selbst ausfallen sollten. Solange die militärische Kommunikationsstruktur erhalten bleibt, ist eine direkte Einflußnahme und damit beispielsweise eine abgestufte Kriegsföhrung (flexible response) möglich, wenn jedoch die Zentren ausfallen, wird automatisch – durch das *Ausbleiben* von Informationen, nicht durch das *Senden* von Information – ein massiver Gegenschlag ausgelöst. Da die Sowjetunion über diesen Tatbestand informiert ist, wird sie sich also hüten, beispielsweise sofort den Präsidenten und den JCS (Joint Chief of Staff) auszuschalten, da dies einen unmittelbaren massiven Gegenschlag bewirken würde (statt eines möglicherweise abgestuft „führbaren“ Krieges).

Dieser Gedanke des Ausbleibens von Information als Auslöser, der hier dem Gesamtsystem zugrunde liegt, wird zum Teil auch für einzelne technische Waffensysteme angewendet (allerdings nicht im Frieden): Nicht der Empfang eines bestimmten Codes wirkt als Auslöser, sondern das Ausbleiben dieses Codes [5].

3. Komponenten und Funktionsweise eines FWES

Das Raketenwarnsystem der USA läßt sich in drei Hauptbereiche einteilen [22]:

- (1) Sensoren zur Feststellung eines Raketenstarts,
- (2) Computerzentren und Kommunikationsnetze zum Analysieren und Weiterleiten der Sensordaten und
- (3) Kommandostellen, in denen die Warninformationen bewertet und angemessene Aktionen angeordnet werden.

3.1. Sensoren zur Feststellung eines Raketenangriffs

Raketenwarnsensoren sind einerseits Infrarotdetektoren, die das brennende Triebwerk einer fliegenden Rakete registrieren und über eine Analyse des Wellenspektrums auch eine Aussage über den Raketentyp selbst ermöglichen. Andererseits werden Radarstationen verwendet, um die Flugbahnen zu beobachten und zu berechnen. Zu den Radarstationen gehören:

- Ballistic Missile Early Warning System (BMEWS),
 - Perimeter Acquisition Radar Attack Characterization System (PARCS),
 - PAVE PAWS, ein sog. „phased array radar“-System.
- Interkontinentalraketen (ICBMs) sollen durch BMEWS und PARCS und U-Boot-gestützte Raketen (SLBMs) durch PAVE PAWS festgestellt werden.

Ein dritter Bereich der gegenseitigen Überwachung beruht auf Horschensoren, die in den letzten zehn Jahren über die strategisch wichtigen Teile der Weltmeere verteilt wurden, um die Bewegung von Unterseebooten festzustellen.

Die Sowjetunion hat mehr und mehr U-Boote des Typs Yankee mit Interkontinentalraketen bestückt. Der Standort dieser U-Boote ist erstens ein wichtiger Indikator für einen möglichen Angriff, und zweitens ist dessen Kenntnis natürlich wichtig für gezielte Gegenmaßnahmen. Diese Information wird durch ein ungeheuer komplexes Überwachungssystem, die sog. Fleet Ocean Surveillance Information Centres (FOSIC) der USA, gesammelt. Die Information selbst liefern Satelliten, Schiffe, Aufklärungsflugzeuge, Agenten und das maritime SOSUS-Netzwerk (US Navy's Sound Surveillance System) [5].

3.2. Computerzentren und Kommunikationsnetze

Die Daten der Sensoren werden unter anderem im 427M-Computersystem der NORAD-Kommandostelle, die in den Cheyenne Mountains in Colorado liegt, verarbeitet. Das 427M-Computersystem besteht aus 84 Computern und über 10 Millionen Zeilen Software-Instruktionen [18] und kann in drei wesentliche Bestandteile eingeteilt werden:

„*Communication System Segment*“ (CSS): Die Kommunikationsstruktur des amerikanischen Raketenwarnsystems wird im wesentlichen durch CSS geliefert. Das CSS bildet die Verbindungsstelle zwischen allen externen Einrichtungen (den Kommandostellen) und den Sensoren. Alle Meldungen werden von CSS vollständig verarbeitet, formatiert, in bestimmten Code convertiert und weitergesendet. CSS kontrolliert die gesamte Kommunikation und ist damit das kritischste Element des 427M-Computersystems. Um höhere Verfügbarkeit zu gewährleisten, besteht CSS aus zwei Computern, einer verarbeitet die Live-Daten, der andere läuft im Backup-Mode als Reserve.

„*NORAD Computer System*“ (NCS): Das NCS liefert zentrale Kommando- und Kontrollinformationen für NORAD. Die wesentlichen, äußerst zeitkritischen Funktionen des NCS sind Empfang, Verarbeitung, Darstellung und Ausgabe von Raketenwarnsignalen, Nuklear-Detonationsberichten, Zustandsberichten von Waffen und Sensoren und die Luftraumüberwachung.

„*Space Computational Center*“ (SCC): SCC ist die amerikanische Zentrale für das Entdecken und Verfolgen aller Satelliten im Weltall. Dazu gehören Start, Einbringen und Verlassen von Umlaufbahnen, Manöver, Zerstörungen und mögliche Aufschlag-Vorhersagen. Die Entwicklung von Satelliten-Angriffs-Warnsystemen, die Unterstützung von Weltraumverteidigungswaffen und die Betreuung von Weltraumfähren gehören ebenfalls zu den Aufgaben des SCC.

Ein weiteres Zentrum der Informationsverarbeitung und Bewertung ist SAC (Strategic Air Command), das teilweise unabhängig von NORAD arbeitet [5]. Ebenso wird im National Military Command Centre, NMCC, das direkt dem Präsidenten untersteht, Information computergestützt gesammelt und bewertet.

Die diesen Zentren zugeleitete Information wird in den großen computergestützten Kommunikationsnetzwerken und Sensornetzen gesammelt, die sich aus den Informationssystemen der Air Force der 50er Jahre entwickelt haben (siehe [5], Kap. 2). Diese militärischen Kommunikationsnetzwerke sind jedoch – selbst wenn sie gegen den EMP gehärtet sind – sehr verwundbar und daher im Ernstfall möglicherweise unzuverlässig. Da die völlige Unzerstörbarkeit eines Kommunikationsnetzes nicht zu erreichen ist, wurde das Problem der Sicherheit durch weitgehende Redundanz gelöst: Im Ernstfall werden die privaten Telefonnetzwerke der USA dem Militär übergeben [5]. Diese Telefonnetze sind so ausgelegt, daß die Informationsverarbeitung auch dann noch möglich ist, wenn große Teile des Netzes ausfallen: In den computergestützten Zentren wird automatisch ein freier Weg durch das verbleibende Netz gesucht.

3.3. Kommandozentralen

Die wichtigsten Kommandozentralen sind:

- North American Aerospace Defense Command (NORAD),
- Strategic Air Command (SAC),
- National Military Command Center (NMCC, Pentagon),
- Alternate National Military Command Center (ANMCC, Fort Ritchie, Maryland),
- Pacific Command (PAC),
- Atlantic Command (LANT),
- European Command (EUR).

Die Daten der Satelliten und PAVE-PAWS-Radar-Stationen, also der Sensoren, die U-Boot-gestützte Raketen registrieren, werden direkt in die ersten vier (amerikanischen) Kommandostellen geleitet [22]. Die Analyse der Sensordaten wird in dem Computersystem von NORAD durchgeführt und von dort an die übrigen Kommandostellen weitergeleitet. Die Daten aller übrigen Sensoren werden nur an NORAD gesendet und von dort an die übrigen Kommandostellen übermittelt.

Die wichtigste (jedoch nicht die einzige) Kommandozentrale ist daher NORAD, wo alle Daten der Sensoren empfangen und ausgewertet werden. Die Aufgaben von NORAD sind im einzelnen [18]:

- Warnung vor möglichen Angriffen von Bombern oder ballistischen Raketen auf Nordamerika,
- Weltraumüberwachung, Verfolgung und Katalogisierung aller künstlichen Objekte im Weltall,
- Luftraumüberwachung, Entdecken und Identifizieren aller Flugzeuge,

– Leitung und Kontrolle der U.S.-amerikanischen und kanadischen Luftverteidigungstreitkräfte. NORAD ist auch dafür verantwortlich, alle weltweiten Raketenstarts und Nuklearevents zu melden; dies gilt auch für den Pazifik und Europa.

Neuere Aufgaben von NORAD umfassen Satelliten-Angriffswarnungen, die Überprüfung aller amerikanischen Satelliten und die Unterstützung der Flüge von Weltraumfähren.

4. Fehlermöglichkeiten und dokumentierte Fehlalarme

In einem so hochkomplexen System wie dem im letzten Abschnitt beschriebenen treten ständig Fehler auf, die unter anderem bedeuten können, daß ein gegnerischer Raketenanflug gemeldet wird, obwohl tatsächlich kein Angriff vorliegt. Wird ein solcher Fehler nicht rechtzeitig erkannt, kann dies zu gefährlichen Situationen und unter gewissen Umständen sogar zum Atomkrieg führen. Selbst wenn diese Fehler rechtzeitig entdeckt werden, können kritische Situationen oder internationale Krisen entstehen:

„Falsche Raketenwarnmeldungen, gesendet von dem 427M-Computersystem, zogen nicht nur die Aufmerksamkeit der gegnerischen Propaganda auf sich, sondern verursachten beinahe eine internationale Krise“ [18].

In diesem Abschnitt werden potentielle Fehlerquellen eines FWES untersucht und einige der dokumentierten Fehlalarme angegeben (4.5.). Zum Vergleich werden zunächst einige bekanntgewordene Fehler aus anderen technischen Systemen beschrieben.

4.1. Fehler in technischen Systemen

In allen Bereichen des technischen Lebens treten Unfälle durch Versagen eines Teils der Technik oder durch Versagen von Menschen in der Beherrschung dieser Technik auf. Diese Unfälle sind oft mit Verlust von Menschenleben verbunden. Beispielsweise entgleisen Züge, Brücken stürzen ein, giftige Gaswolken entweichen ins Freie und Flugzeuge stürzen ab. Hinterher kann oft bis ins Detail geklärt werden, warum es zu diesem Unfall gekommen ist: Meistens hat eine unglückliche Verkettung von unwahrscheinlichen Zufällen zu solchen Unfällen geführt. Diese potentielle Fehlermöglichkeit hat oft lange bestanden, ohne daß etwas passierte. Ein Chemiewerk kann noch so lange fehlerfrei arbeiten, dadurch wird die Wahrscheinlichkeit, daß irgendwann eine tödliche Gaswolke ins Freie gelangt, nicht geringer.

In vielen Fällen sind die Folgen eines Unfalls in einem technischen System so schwerwiegend, daß von vornherein alle erdenklichen Maßnahmen getroffen werden, um solche Unfälle zu verhindern. Dies gilt besonders im nuklear-militärischen Bereich, also auch für

Frühwarn- und Entscheidungssysteme, es gilt beispielsweise aber auch bereits für die Stromversorgung und für Kernkraftwerke.

Wegen der ernsten Folgen, die der Zusammenbruch eines Stromversorgungsnetzes haben kann, wurden in den USA Vorkehrungen getroffen, um solche Unfälle zu verhindern. Das System war zum Beispiel so konstruiert, daß es einen Blitzschlag absorbieren konnte, gleich an welcher Stelle er auftrat. 1965 kam es aber trotzdem zum Zusammenbruch der Stromversorgung im ganzen Nordwesten der USA sowie in Teilen von Kanada: Es schlugen Blitze an verschiedenen Stellen des Systems fast gleichzeitig ein [15]. Mit einem solchen Fall hatte man beim Entwurf des Systems nicht gerechnet. Nach der Untersuchung dieses Vorfalls wurde immer wieder versichert, daß Änderungen am System vorgenommen wurden, die es unmöglich machen, daß ein solcher Unfall noch einmal passiert [16]. Doch im Juli 1977 geschah der gleiche Unfall nochmals in New York [8, 13].

Der Unfall im Kernkraftwerk „Three Mile Island“ von 1979 geschah, nachdem unzählige technische Studien über die Sicherheit des Kernkraftwerks durchgeführt worden waren. Kernkraftvertreter hatten erklärt, daß es sehr viel wahrscheinlicher sei, von einem Meteor erschlagen zu werden, als daß ein gravierender Unfall im Kernkraftwerk passiert. Der Unfall in Three Mile Island begann mit einem Gerätefehler. Anschließend Bedienungsfehler verursachten die Stärke und die gravierenden Folgen des Unfalls, die zum teilweisen Durchschmelzen des Kerns (ein Unfall, der als unmöglich galt) führten [26].

Das Problem liegt unter anderem in der Analyse der Fehlerwahrscheinlichkeit: Aus der Fehlerwahrscheinlichkeit der einzelnen Komponenten wird auf die Fehlerwahrscheinlichkeit des gesamten Systems geschlossen. Dabei bleibt dann unberücksichtigt, daß es eine unglückselige, *nicht vorhergesehene* Verkettung von Ursachen geben kann, die aller Analyse zum Trotz doch einen Fehler auslöst.

4.2. Fehler im Datenfluß eines FWES

In jedem Stadium der gesamten Informationsverarbeitung und in jeder Komponente eines informationsverarbeitenden Frühwarn- und Entscheidungssystems können Fehler auftreten. Im informationsverarbeitenden Prozeß eines FWES sind zum Beispiel folgende Fehlertypen möglich [21, 28]:

- Erfassung von Primärdaten über fliegende Objekte: Da der Luftraum zunehmend militärisch und zivil genutzt wird, gilt es, ständig eine breite Palette „irrelevanter“ Daten auszuwerten. Hierbei können sich Fehler ergeben, wie sie zum Beispiel aus der zivilen Flugüberwachung wohlbekannt sind und dort häufig zu Beinahezusammenstößen geführt haben.
- Auswertung und Interpretation der Primärdaten zu Tracks:

Zur Interpretation von Flugbahndaten und primären Kennwerten über fliegende Objekte werden Entscheidungstabellen verwendet, die in der Regel unvollständig sind, da immer wieder neue Objekte auftauchen. Selbst bei den heute schon zu klassifizierenden fliegenden Objekten macht deren hohe Zahl Fehler recht wahrscheinlich. Insbesondere kann die Zerstörung eines Sensors, zum Beispiel eines militärischen Beobachtungs-Satelliten durch eines von ca. 5000 zur Zeit im Umlauf befindlichen künstlichen Objekten im Weltall, leicht als wichtiges Primärdatum gewertet werden, als Beginn eines Krieges etwa, der heute wahrscheinlich mit der Zerstörung der Kommunikationsstruktur beginnen wird.

- **Telekommunikation:**

Trotz hoher Redundanz in den militärischen Telekommunikationssystemen (Sicherung der Übertragung, mehrere parallele Systeme für eine Übertragung) sind Fehler nicht ausgeschlossen, sie können (a) von der primären Eingabe in den betreffenden Kontrollzentren, (b) von Störungen in der Auswertung oder (c) von Übertragungsproblemen herrühren. Insbesondere kann die automatische Verarbeitung und Verschlüsselung von Nachrichten auf den Kommunikationsstrecken durch Hardware- und Softwarefehler zu Problemen führen.

- **Befehlsübertragung und Ausführung:**

Obwohl durch komplexe „Schlüssel“ ein „Raketenstart aus Versehen“ sehr unwahrscheinlich ist, kann natürlich im Krisenfall, wo Nachrichten über anfliegende atomare Raketen vielleicht bei den Bodenstationen bekannt sind, eine menschliche Fehlreaktion nicht ausgeschlossen werden.

4.3. Computerfehler

Für den Betrieb von Frühwarn- und Entscheidungssystemen sind Fehler, die den Ausfall oder das Anhalten einer Computeranlage verursachen, nicht sehr problematisch. Gefährlich können Fehler dann werden, wenn sie zum Aussenden von falschen Informationen führen. Wie auch aus den dokumentierten Fehlern in 4.5 hervorgeht, können solche gefährlichen Fehler in Computeranlagen als Hardware-, Software- oder Entwurfsfehler auftreten.

Fehler in der Hardware einer Computeranlage sind das Versagen eines Chips oder eines anderen Bauelements, wie das beispielsweise bei dem Fehlalarm am 3.6. 80 (siehe 4.5) aufgetreten ist. Solch ein Hardwarefehler kann z. B. durch lokale Überhitzung von Bauelementen oder durch Fehler bei der Reparatur und dem Auswechseln von elektronischen Komponenten entstehen.

Häufiger als Hardwarefehler sind Softwarefehler, also Fehler in der Programmierung. In der Informatik wurden viele Methoden entwickelt, um bei der Programmierung von komplexen Systemen die Zahl der Softwarefehler möglichst gering zu halten. Einige dieser

Methoden sind disziplinierte Top-Down-Entwicklung, Verwendung von mehreren simultanen Anlagen oder die Programmverifikation.

Bei den Softwarefehlern sind die logischen Fehler, die beim Entwurf (der Spezifikation) eines Systems gemacht werden, besonders schwerwiegend, denn sie treten danach in jeder Programmierung auf, die sich an diese Spezifikation hält, und sind für den Benutzer nicht unmittelbar erkennbar. Sie führen in der Regel zu einem falschen Verhalten des Programms und zu falscher Information, geben dies aber nicht unmittelbar zu erkennen.

Die Spezifikation eines Programmsystems ist eine Beschreibung der Aufgaben, die von dem Computer ausgeführt werden sollen. Die Spezifikation, die für komplexe Systeme äußerst kompliziert und umfangreich wird, kann nun etwas ausdrücken, was vom Sinn her ganz anders gemeint war, oder es können wichtige Aspekte vergessen werden. Eine Spezifikation, die solche Fehler enthält, ist nicht „falsch“, sondern beschreibt eine andere Aufgabenstellung, als der Benutzer ursprünglich im Sinn hatte. Solche Fehler sind mit Mitteln der Informatik prinzipiell nicht zu vermeiden.

Beispielsweise können, ausgehend von einer Spezifikation, mehrere unabhängige Softwaregruppen unabhängige Implementierungen (Programmsysteme) entwickeln, die dann simultan auf verschiedenen Computeranlagen ablaufen. Bei abweichendem Verhalten eines Programms durch Programmierfehler kann der Ablauf nach Mehrheitsentscheid fortgeführt werden, ohne daß diese Fehler irgendwelche Auswirkungen hätten. Durch diese Methode wird die Fehlerhäufigkeit zweifellos verringert, aber Fehler in der Spezifikation schlagen sich in alle Implementierungen durch und werden deshalb nicht erkannt. Das gleiche gilt für die Programmverifikation und für den Einsatz mehrerer Computer im Tandem-Betrieb, wie zum Beispiel im Space-Shuttle-Programm: Dort kam es trotzdem zu so massiven Fehlern, daß ein Flug abgesagt werden mußte.

Insgesamt ist unter Informatikern unumstritten, daß zum heutigen Zeitpunkt und in absehbarer Zukunft Programme nicht fehlerfrei oder innerhalb einer vorgeschriebenen Fehlerwahrscheinlichkeit erstellt werden können.

Ein wichtiges Hilfsmittel zur Fehlersuche in Computersystemen ist daher das Testen. Ein Frühwarn- und Entscheidungssystem kann aber nicht unter realen Bedingungen getestet werden, das heißt, es kann kaum festgestellt werden, wie sich das System in nicht vorhersehbaren künftigen Situationen, insbesondere in Krisen- oder Konfliktzeiten, verhält.

4.4. Menschliche Fehler

Bei Anzeichen einer Bedrohung durch atomare Interkontinentalraketen stehen der Bedienungsmannschaft eines Raketenwarnsystems etwa 30 Minuten zur Verfüg-

gung, um eine solche Information auf Echtheit zu überprüfen. Durch das Zusammenrücken der sich in Europa gegenüberstehenden Raketen und die zunehmende Stationierung von atomaren Raketen auf U-Booten schwindet die Zeit, die der Kontrollmannschaft zur Überprüfung von Alarmmeldungen übrig bleibt, auf wenige Minuten.

Die möglicherweise schwerwiegenden Entscheidungen, die von den Menschen dann in aller kürzester Zeit gefordert sind, verursachen einen enormen Streß, so daß es fraglich ist, ob in solchen Situationen noch sinnvolles und korrektes Handeln möglich ist. Die Menschen müssen sich in ihren Entscheidungen zunehmend auf die Informationen, die ihnen die Computer liefern, verlassen.

Neben der Gefahr von menschlichem Fehlverhalten wegen einer Überforderung durch Streß und Zeitnot können auch Gefährdungen durch Fahrlässigkeit oder mutwillige Manipulation entstehen.

Dumus berichtet in [11], daß beispielsweise im Zeitraum 1975 bis 1977 etwa 5000 Personen jährlich wegen Alkohol- und Drogenmißbrauchs, wegen Geistesstörungen, unnormalem Verhalten und anderer Verfehlungen aus den Nuklearstreitkräften entfernt wurden.

Es ist damit zu rechnen, daß diese Faktoren die Reaktion der Menschen so beeinflussen können, daß sie in ihrem Kompetenzbereich unkontrolliert und fahrlässig handeln, mit unter Umständen gravierenden Folgen.

Daneben ist auch nicht auszuschließen, daß es – unter den genannten wie natürlich auch unter den nicht besonders auffälligen Mitarbeitern – Menschen gibt, die bewußt Manipulationen während des Betriebs an einer Einheit eines FWES vornehmen, als Scherz, aus Rache oder aus politischen Gründen. Solche Sabotage kommt im zivilen Bereich häufig zum Beispiel in Form von Brandstiftungen vor. Da es in hochkomplexen Systemen nicht möglich ist, daß einige wenige Personen das gesamte System verstehen, sind viele Menschen nötig, um Wartung und Reparaturen durchführen und den Betrieb aufrechterhalten zu können. Dieser gesamte Personenkreis ist potentiell in der Lage, bewußt unerlaubte Manipulationen vorzunehmen, und es ist sicher schwierig, Maßnahmen zu ergreifen, die diese Gefahr ausschließen.

4.5. Dokumentierte Fehlalarme

In den Jahren 1979–1981 gab es etliche Presseberichte über Fehlalarme, die von NORAD verursacht wurden. Dies führte dazu, daß der amerikanische Senat einen Untersuchungsausschuß bildete. In dessen Bericht an den Senat [22] und in [18] sind für den Zeitraum vom 1.1. 79 bis 30.6. 80 147 irrtümliche Fälle von Anzeichen einer Bedrohung des nordamerikanischen Kontinents angegeben, die zur Auslösung der ersten Alarmstufe führten (Missile Display Conference). Die folgenden fünf Fälle führten zur zweiten Alarmstufe (Threat Assessment Conference):

3. Okt. 1979: Ein Radar, zuständig zum Erfassen U-Boot-gestützter ballistischer Raketen, entdeckte einen auf einer niedrigen Umlaufbahn fliegenden Raketenkörper, der kurz vor dem Auseinanderbrechen war, verursachte einen falschen Alarm und eine Treffermeldung.

9. Nov. 1979: Anzeichen eines Massenüberfalls wurden dadurch verursacht, daß ein Simulationsprogramm zum Testen irgendwelcher Systemkomponenten in das Raketenwarn-Computersystem von NORAD eingeführt wurde, ohne daß das Bedienungspersonal an den Bildschirmen davon Kenntnis hatte.

15. März 1980: Im Rahmen sowjetischer Übungen wurden vier auf U-Booten stationierte ballistische Raketen aus dem Gebiet der Kurilen gestartet. Einer dieser Starts entwickelte eine Flugbahn, die einen Angriffspunkt in den USA zu ergeben schien.

3. und 6. Juni 1980: Durch einen Hardwarefehler eines „communication multiplexers“ wurden Fehlalarme verursacht. Der „communication multiplexer“ ist Teil des Kommunikationssystems bei NORAD und enthält auf der Basis der Analyse von Sensordaten Meldungen, die an die anderen Kommandostellen gesendet werden. Um ständig die Leitung überprüfen zu können, werden die Meldungen permanent gesendet, wobei normalerweise in dem Teil der Meldungen, der die Anzahl entdeckter Raketenstarts übermittelt, nur Nullen stehen. Der Hardwarefehler äußerte sich nun dadurch, daß einige dieser Nullen durch positive Zahlen überschrieben wurden. Dadurch meldete NORAD einen sowjetischen Massenangriff an die anderen Kommandostellen.

Nach diesen Fehlern wurden enorme Anstrengungen unternommen, um die aufgetretenen Mängel zu beseitigen. Diese Maßnahmen werden in einem Bericht des General Accounting Office [18] aufgelistet; die Autoren kommen jedoch abschließend zu der kritischen Einschätzung:

„Fehlerhafte Anzeichen von Raketenstarts können immer wieder vorkommen, da kein System gebaut werden kann, das alle Sonderfälle berücksichtigt“ ([18], S.4).

5. Maßnahmen bei einem Alarm

Die amerikanischen Senatoren Hart und Goldwater beschreiben in dem erwähnten Bericht an den Senat [22], welche Maßnahmen getroffen werden, wenn Anzeichen einer wirklichen Bedrohung oder zweifelhafte Daten vorliegen. In solchen Fällen starten die vier wichtigsten Kommandostellen ein offizielles Konferenzverfahren, um die Situation zu beurteilen. Drei Arten von Konferenzen können einberufen werden:

- Missile Display Conference,
- Threat Assessment Conference,
- Missile Attack Conference.

Missile Display Conference

Werden an irgendeiner Stelle des Raketenwarnsystems zweifelhafte Daten festgestellt, dann wird als erstes eine „Missile Display Conference“ einberufen. Solche zweifelhaften Daten stammen in den meisten Fällen von den Sensoren. Beobachten die Satelliten ein Infrarotsignal, dann wird dieses mit den Infrarotsignalen, die früher bei sowjetischen Raketen beobachtet wurden, verglichen. Aber es gibt auch andere physikalische Phänomene, sowohl in der Atmosphäre als auch auf der Erdoberfläche, die ähnliche Infrarot-Signale erzeugen. Das Sensorsystem muß einerseits empfindlich genug sein, um jeden Raketenstart zu registrieren, und es darf andererseits das System nicht mit irrelevanten Informationen überladen. Diese Balance zu erreichen, ist ein fortwährendes Problem, und in der Missile Display Conference müssen ständig solche Signale beurteilt werden um nachzuweisen, daß es sich nicht um eine Bedrohung durch Raketen handelt.

Außerdem werden routinemäßig Missile Display Conferences abgehalten, wenn die Position oder Konfiguration eines Sensors geändert wird, wodurch ungewöhnliche Informationen in das System gelangen könnten.

1979 gab es 1544 routinemäßige Missile Display Conferences, die zu dem Ergebnis kamen, daß keine akute Bedrohung vorlag. 78 solcher Konferenzen hielten Anzeichen einer Bedrohung des nordamerikanischen Kontinents für möglich. Im ersten Halbjahr 1980 fanden 2159 routinemäßige Missile Display Conferences statt, ausgelöst durch die Warnsensoren, die bestimmte physikalische Phänomene falsch identifizierten, oder die durch die Rekonfiguration der Sensoren notwendig wurden. 69mal mußten Anzeichen einer möglichen Bedrohung beurteilt werden.

„Für das Raketen-Warn-System ist es ein alltägliches Problem, falsche Anzeichen eines Angriffs von potentiell richtigen Anzeichen eines Angriffs zu unterscheiden“ [22].

Die „Missile Display Conference“, die erste Stufe der Bewertung von Sensordaten, ist beendet, wenn der „Commander-in-Chief“ von NORAD die Entscheidung trifft, daß alle verfügbaren Daten entweder die Anwesenheit oder die Abwesenheit eines Angriffs auf Nordamerika anzeigen.

Threat Assessment Conference

Falls der NORAD-Kommandeur die Möglichkeit einer Bedrohung feststellt, wird als nächster Schritt die „Threat Assessment Conference“ einberufen. Diese bezieht ranghöhere Personen der verschiedenen Kommandostellen, z. B. den „Chairman of the Joint Chiefs of Staff“, mit in die Bewertung ein. Die Aufgabe dieser Konferenz ist es festzustellen, welcher Art die Bedrohung Nordamerikas ist, und Maßnahmen zu treffen, um die Funktionsfähigkeit der Streitkräfte zu gewähr-

leisten. 1979 und 1980 wurde fünfmal eine Threat Assessment Conference einberufen, und zwar in den in Abschnitt 4.5 angegebenen Fällen.

Missile Attack Conference

Falls die Bedrohung bestehen bleibt, wird als letzter Schritt die „Missile Attack Conference“ einberufen, die die ranghöchsten Personen einbezieht, einschließlich des Präsidenten der USA. Nach dem Bericht von Hart und Goldwater trat eine solche Konferenz bisher noch nicht zusammen [22].

Am Beispiel des Alarms vom 3. Juni 1980 wird der Ablauf der beiden ersten Konferenzen (Alarmstufen) in [22], S. 5, wie folgt beschrieben:

„Am 3. Juni 1980 um 2 Uhr 26 zeigen die Bildschirme der SAC-Kommandostelle einen Start von zwei U-Boot-gestützten Raketen in Richtung USA an. 18 Sekunden später zeigen die Anzeigesysteme eine wachsende Anzahl von U-Boot-Raketenstarts an. Das SAC-Kommandostenpersonal ruft die NORAD-Kommandostelle an. Das NORAD-Personal gibt an, daß keine Anzeichen eines Raketenstarts vorliegen. Kurz nach den ersten Hinweisen auf Raketenstarts ordnet der „duty controller“ von SAC an, daß sich die Bereitschaftspiloten in ihre Flugzeuge begeben und die Motoren anlassen, um einen Start vorzubereiten.“

Nach kurzer Zeit sind die Anzeichen drohender U-Boot-Raketen auf den SAC-Bildschirmen verschwunden. NORAD berichtet, daß keine Raketensignale von den Sensoren kommen und daß keine Daten an SAC, NMCC oder ANMCC gesendet werden. Kurz danach werden die SAC-Flugzeugbesatzungen angewiesen, die Motoren auszuschalten, aber in ihren Flugzeugen zu bleiben. NORAD berichtet, daß alle Systeme in Ordnung sind. Kurz danach zeigen die SAC-Bildschirme an, daß sowjetische Interkontinentalraketen in Richtung USA gestartet worden sind. Nach einer Pause erhält die NMCC-Kommandostelle Anzeichen, daß U-Boot-Raketen in Richtung USA gestartet worden sind.

Alle Hinweise auf drohende Raketen in den Kommandostellen SAC und NMCC stammten aus dem NORAD-Kommunikationssystem CSS und kamen nicht direkt von den Sensoren.

Der NMCC-„Duty Officer“ beruft eine „Missile Display Conference“ ein, um die Situation zu bewerten. Die Konferenz bleibt bestehen, während die vier Kommandostellen versuchen, den Ursprung für die Daten festzustellen.

Der NMCC-„Duty Officer“ beruft eine „Threat Assessment Conference“ ein. Als Teil der Standardreaktionen bei einer Threat Assessment Conference bereitet die Luftkommandostelle des „Pacific Command“ ihren Start vor. Kurze Zeit später bestätigt der Kommandeur von NORAD, daß keine Bedrohung vorliegt. Als Reaktion auf die dennoch andauernde Threat Assessment Conference startet die Luftkommandostelle. Dann beendet der NMCC-„Duty Officer“ die Threat Assess-

ment Conference. Eine Minute später beendet SAC ihren Alarm, und die Alarmmannschaften kehren in ihre Unterkünfte zurück.“

6. Bewertung und Wirkung eines Fehlalarms

6.1. Ungewöhnliche Fehler

Die Kontrollmannschaft bei NORAD muß täglich zweifelhafte oder fehlerhafte Daten bewerten, von denen einige Tausend pro Jahr zum Einberufen der „Missile Display Conference“ führen. Obwohl diese Daten teilweise Indizien für Raketenangriffe auf Nordamerika sein könnten (78mal im Jahr 1979 und 69mal im ersten Halbjahr 1980), führten sie lediglich zur ersten Konferenz- und Alarmstufe ([22], S. 4).

Dagegen wurde bei dem Fehlalarm vom 3. Juni 1980 eine „Threat Assessment Conference“ einberufen (Alarmstufe 2), die Flugzeugbesatzungen wurden in Alarmbereitschaft versetzt, und eine Luft-Kommandostelle war bereits gestartet, obwohl das Personal der Kommandostellen sehr schnell überprüfen konnte, daß es sich hier um fehlerhafte Daten handeln mußte, denn

1. es gab keine Sensorsignale über irgendwelche Raketen,
2. die Hinweise auf den Bildschirmen, die von NORAD empfangen wurden, entsprachen keinem logischen Muster und bildeten keine Folge von Ereignissen, wie sie bei einem Raketenstart erwartet würde, und
3. die verschiedenen Kommandostellen erhielten unterschiedliche Hinweise auf eine Bedrohung.

Trotzdem hatte dieser Fehlalarm in den Kommandostellen einige Aufregung verursacht ([22], S. 4).

Die sehr häufig auftretenden Sensorsignale von bisher nicht bekannten Flugobjekten, die fälschlicherweise Hinweise auf Raketenangriffe liefern, werden offenbar vom Personal der Kommandostellen sehr viel leichter korrekt bewertet als selten auftretende Fehlerarten wie die vom 3. Juni 1980.

Eine Verringerung der Fehlerhäufigkeit durch ausgefeiltere technische Methoden erhöht also nicht notwendig die Sicherheit, denn gerade selten oder erstmals vorkommende Fehlerarten sind vom Bedienungspersonal besonders schwer zu beurteilen.

6.2. Krisensituation und Zusammentreffen von Ereignissen

Die Maßstäbe zur Bewertung der Alarmsituation, die ein Frühwarn- und Entscheidungssystem auslöst, hängen wesentlich von der weltpolitischen Lage ab. Während die Überprüfung von Alarmmeldungen in Friedenszeiten von vornherein eher darauf abzielt, diese als Fehlalarm zu erkennen, ändert sich die Strategie in Zeiten schwerer politischer Krisen oder Konflikte. Der Informationsfluß der weltweiten elektronischen Sensoren und Warnsysteme, der in die Kommandozentralen ein-

strömt, wächst derart stark an, daß eine genaue Überprüfung von Ereignissen und Alarmmeldungen nur in geringerem Umfang möglich ist, und die Schwelle, ab der die Alarmmeldungen für echt gehalten werden, wird sehr viel niedriger.

Wie im Abschnitt 4.1 bemerkt, wird die Wahrscheinlichkeit für einen schweren Unfall in einem komplexen technischen System dann besonders groß, wenn mehrere Ereignisse oder Fehler zufällig zusammentreffen, da dann die Anzahl möglicher Situationen und etwaiger Reaktionen zu groß wird, als daß man sie schon beim Entwurf des Systems berücksichtigen könnte. Zudem sind auch für Menschen solche Situationen äußerst schwer zu beurteilen, so daß es leicht zu Fehleinschätzungen und Fehlreaktionen kommen kann.

Im militärischen Bereich kann das zufällige Zusammentreffen mehrerer unabhängiger Ereignisse mitten in einer politischen Krise zu äußerst gefährlichen Situationen führen, wie das folgende Beispiel zeigt ([5], S. 65):

„Im frühen November 1956, zur gleichen Zeit, als die Briten und Franzosen in Suez eingriffen, fand die Besetzung Ungarns statt. TASS, die sowjetische Nachrichtenagentur, erzeugte die Angst vor einem weltweiten Nuklearkrieg. Moskau sandte eine amtliche Verlautbarung an London und Paris, mit klaren Andeutungen, daß Raketenangriffe gegen diese Städte in Betracht gezogen würden. In einer anderen Verlautbarung an Washington schlug Moskau eine gemeinsame amerikanisch-sowjetische Militäraktion in Suez vor. Diese Nachricht wurde im Weißen Haus am späten Nachmittag des 5. November erhalten. Vor diesem Hintergrund trafen in der folgenden Nacht vier Ereignisse zusammen: Die oberste US-Kommandostelle in Europa erreichte eine Blitznachricht, daß nichtidentifizierte Düsenjäger über der Türkei fliegen und die türkische Luftwaffe daraufhin in Alarmbereitschaft versetzt worden sei. Es gab zusätzliche Berichte über 100 sowjetische MIG-15 über Syrien sowie Berichte, daß eine britische Canberra über Syrien abgeschossen worden sei. (Zu dieser Zeit waren nur die sowjetischen MIGs in der Lage, die hoch fliegenden Canberra-Bomber abzuschießen.) Schließlich gab es noch Berichte, daß eine russische Flotte durch die Dardanellen fuhr. Das wurde lange Zeit als ein Zeichen für Feindseligkeiten angesehen, weil die Sowjetunion in Krisenzeiten bestrebt sein mußte, ihre Flotte aus dem Schwarzen Meer zu bringen (in beiden Weltkriegen war sie dort eingeschlossen).“

Die Reaktion des Weißen Hauses auf diese Ereignisse ist nicht vollständig bekannt, doch wird berichtet [14], daß General Goodpaster befürchtete, die Ereignisse könnten die NATO-Einsatzpläne auslösen, die zu jener Zeit einen totalen nuklearen Vergeltungsschlag gegen die Sowjetunion vorsahen.

Im nachhinein entpuppten sich die Düsenjäger über der Türkei als Schwanenschar, die vom Radar erfaßt und falsch identifiziert worden war. Die 100 sowjetischen MIGs stellten sich als eine wesentlich kleinere routinemäßige Begleitung für den syrischen Präsi-

ten heraus, der von einem Staatsbesuch aus Moskau kam. Der britische Canberra-Bomber stürzte aufgrund von technischen Schwierigkeiten ab, und die sowjetische Flotte befand sich in einem lang geplanten Manöver.

Die Wahrnehmung und Mißinterpretation dieser Ereignisse, vor dem Hintergrund der gespannten Weltlage durch Ungarn und Suez, war das erste wichtige Beispiel, wie die Größe und die Komplexität der weltweiten elektronischen Warnsysteme in bestimmten kritischen Zeiten von allein eine Krise auslösen können.“

Die einzelnen Ereignisse waren isoliert betrachtet relativ harmlos, aber durch ihr Zusammentreffen in einer schweren weltpolitischen Krise entstand eine äußerst bedrohliche Situation, die weitaus schlimmer gewesen wäre, wenn statt der MIGs über der Türkei anfliegende Atomraketen von NORAD gemeldet worden wären.

6.3. Alarmierungsketten

Die verzahnte Alarmierungskette der europäischen Armeen, die 1914 zum Ausbruch des Ersten Weltkrieges führte, wurde nach Darstellung einiger Historiker nicht allein durch das Attentat in Sarajevo, sondern durch die Entscheidung zur Mobilisierung ausgelöst. Tausende ausgegebener Befehle bewirkten die Erzeugung einer Kettenreaktion von sich ständig erhöhenden Alarmstufen, die nicht mehr zu stoppen war: Schritt für Schritt bewegte sich Europa unaufhaltsam dem Krieg entgegen. Unfälle waren nicht nötig, um Europa in den Krieg zu treiben, denn die Kriegssysteme jener Zeit versetzten die Nationen gegenseitig in Angst und Schrecken, und die politischen Führer verloren die Kontrolle, als die Armeen in Alarmbereitschaft versetzt wurden.

Die Gefahr, die von einer Alarmierung ausgeht, führte schon oft zu Entscheidungskonflikten in Krisensituationen. Um die Nazis nicht zu provozieren, traf zum Beispiel Stalin 1941 keine Vorkehrungen, seine Armeen zu verstärken, obwohl ihm mehrfach mitgeteilt wurde, daß Hitler beabsichtige anzugreifen. Während der sowjetischen Invasion in der Tschechoslowakei 1968 hatte die NATO alle routinemäßigen Aufklärungsflüge über Westdeutschland gestrichen, um der Sowjetunion nicht den Eindruck zu geben, die NATO würde ihre militärischen Aktivitäten erhöhen.

Die Möglichkeit, Alarmierungsketten zu erzeugen, ist eine enorme Gefahr, die von Fehlalarmen in Frühwarn- und Entscheidungssystemen ausgeht: Beim Fehlalarm vom 3.6. 80 (Abschnitt 5) wurden Bomberbesatzungen und Raketenstellungen in Alarmbereitschaft versetzt, und die Luftkommandostelle auf Hawaii war gestartet. Solche Aktivitäten werden vom Gegner erkannt und können dort, insbesondere in Krisen- oder Konfliktzeiten, ebenfalls zu erhöhter Alarmbereitschaft führen, die wieder Rückwirkungen auf die eigene Beurteilung der Lage hat.

Unzählige Beispiele belegen, wie genau die Ameri-

kaner über Aktivitäten der Sowjetunion informiert sind und umgekehrt. Zum Beispiel kannten die Amerikaner den Funkverkehr zwischen sowjetischen Piloten und Kommandostellen beim Abschub eines südkoreanischen Verkehrsflugzeuges am 1. September 1983 [6]. 1969 schossen die Nordkoreaner ein amerikanisches Aufklärungsflugzeug in internationalem Luftraum ab. Auf einer Pressekonferenz kurz nach diesem Vorfall erklärte der damalige amerikanische Präsident Richard Nixon, die USA hätten gewußt, daß den Nordkoreanern und Sowjets die Position der Maschine im internationalen Luftraum bekannt gewesen war [6].

Zusätzlich zu den verbesserten Möglichkeiten, die feindlichen Streitkräfte zu beobachten (was zu schnelleren Gegenreaktionen führen kann), ist es jetzt durch die Informationssysteme auch möglich, die feindlichen Warn- und Informationssysteme selbst zu beobachten und sogar direkt in das feindliche Informationsnetz einzudringen. Es besteht die Möglichkeit, daß die jeweiligen Warn- und Informationssysteme sich gegenseitig in ungewöhnlicher oder komplizierter, nicht vorhersehbarer Weise beeinflussen und eine Alarmierungskette erzeugen ([5], S. 60).

Die Nuklearstreitkräfte beider Weltmächte können mit ihren Warn- und Informationssystemen als ein einziges sich gegenseitig beeinflussendes komplexes System betrachtet werden, von dem ungewiß ist, wie es sich in Krisen- oder Konfliktzeiten verhalten wird. Insbesondere ist fraglich, ob ein solches System als Ganzes noch von Menschen kontrolliert oder beherrscht werden kann.

7. Launch on Warning

Die militärpolitische Entwicklung der letzten Jahrzehnte basiert auf der „Abschreckungs-Doktrin“, die besagt, daß der Ausbruch eines Atomkrieges dadurch verhindert werden kann, daß derjenige, der einen Atomangriff in Erwägung zieht, genau weiß, er kann den Gegner niemals so vernichtend schlagen, daß dieser nicht mehr zu einem Gegenschlag fähig wäre. Diese Zweitschlagfähigkeit ist derzeit die Grundvoraussetzung für die Gültigkeit der „Abschreckungs-Doktrin“, auf der das Gleichgewicht beruht.

Vor diesem Hintergrund hatten sich beide Weltmächte auf eine Militärstrategie geeinigt, die als „Launch on Impact“ bezeichnet wird. Nach dieser Strategie wird erst dann ein massiver Gegenschlag ausgeführt, wenn nachweislich atomare Raketen des Gegners auf dem eigenen Territorium eingeschlagen sind. Solange diese Strategie für beide Seiten verbindlich ist, ist die Fehleranfälligkeit eines FWES nicht unmittelbar lebensbedrohend: Selbst wenn irrtümlich ein gegnerischer Raketenangriff gemeldet wird, würde dies zunächst zu einem erhöhten Alarmzustand führen, jedoch nicht zum Start der eigenen Raketen.

Diese Strategie des „Launch on Impact“ kann jedoch nur so lange von beiden Seiten aufrecht erhalten

werden, wie jeder über eine gesicherte Zweitschlagfähigkeit verfügt, d.h. trotz der ungeheuren Verwüstungen, die ein atomarer Angriff auslösen würde, können immer noch so viele eigene Raketen gestartet werden, daß der Gegner vernichtet werden kann. Insbesondere bedeutet dies, daß die militärische Infra- und Kommandostruktur auch nach einem gegnerischen Raketenangriff in wesentlichen Teilen funktionsfähig bleiben muß.

Durch die hohe Treffsicherheit der neuen Waffen ist dieser letzte Punkt zweifelhaft geworden: Zum Beispiel hat die U.S. Minuteman III Mk 12 eine Zielgenauigkeit von 280 Metern, während die älteren Titan-II-Raketen nur im Umkreis von 1300 m trafen. Die neuen sowjetischen SS-18-Mod3-Raketen haben eine Zielgenauigkeit von 350 m, die alten SS-11-Mod1-Raketen 1400 m [24].

Die derzeit entwickelten und zum Teil schon aufgestellten Waffen – z. B. die Pershing-II-Raketen – haben noch eine erheblich größere Zielgenauigkeit, die im Bereich von 10 bis 50 m liegt. Während die Raketen der alten Generation auf einer ballistischen Kurve ihr Ziel erreichen und die Genauigkeit also ausschließlich zum Zeitpunkt des Abschusses kontrolliert werden muß, ist dies bei den neuen Waffen nicht mehr der Fall: Die Pershing-II-Rakete wird zunächst wie eine herkömmliche Rakete auf eine ballistische Bahn mit dem ungefähren Zielpunkt geschossen, aber auf dem letzten Teil der Bahnkurve übernimmt ein eingebauter Bordcomputer selbständig die Zielkorrektur. Dazu wurde das Gelände um das Ziel vorher durch Aufklärungsflüge erkundet und aufgenommen und dem Bordcomputer eingespeist. Durch den Vergleich dieser Daten mit den Daten, die eine eingebaute Radarkamera während des Fluges aufnimmt und an den Computer weitergibt, können dann bis zum Aufschlag automatisch Kurskorrekturen vorgenommen werden.

Noch weiter geht die automatische Steuerung der Cruise Missiles, die während ihrer gesamten Flugzeit durch den Bordcomputer gesteuert werden und das Gebiet ihrer Flugstrecke, das durch hochfliegende Spionageflugzeuge oder Satelliten vorher aufgenommen und vermessen wurde, vollständig einprogrammiert haben.

Diese neuen Waffen, die mit Hilfe von Mikroelektronik selbsttätig ihr Ziel finden und die alten Waffen nach und nach verdrängen werden, stellen eine völlig neue Bedrohung dar: Durch die hohe Zielgenauigkeit können Raketensilos und Kommandozentralen mit einer bisher unerreichbar hohen Trefferwahrscheinlichkeit ausgeschaltet werden [25].

Unter dem Einfluß der neuen Technologien und der damit verbundenen Bedrohung haben beide Großmächte eine Infrastruktur aufgebaut, die es ihnen gestattet, jederzeit zu einer „Launch-on-Warning“-Strategie überzugehen, d.h. bereits dann den Gegenschlag anzuordnen, wenn die Frühwarnsysteme einen massiven Angriff des Gegners melden [5].

In der Tat haben auch beide Seiten angekündigt, die Anwendung einer solchen Strategie zu erwägen:

„Launch-on-Warning“-Vorschläge in den USA

R. Garwin, ein bekannter Physiker und militärischer Berater, schlägt in „Launch under Attack to Redress Minuteman Vulnerability“ [17] vor, eine beschränkte Anzahl von etwa 50 Minuteman-Raketen bereits dann zu starten, wenn die Frühwarnsysteme einen Angriff melden. Diese Raketen sollten erst während des Fluges durch einen Computerbefehl scharf gemacht werden, oder sie könnten umgekehrt bereits feuerbereit gestartet werden, jedoch mit einem technischen Gerät ausgestattet werden, das die Detonationsfähigkeit während des Fluges wieder ausschaltet, falls sich der Alarm als Irrtum herausstellen sollte.

Ähnliche „Launch-on-Warning“-Vorschläge werden zum Beispiel in [12] und in [30] diskutiert, für weitere Zitate und bibliographische Hinweise siehe [4].

Im Zusammenhang mit der öffentlichen Diskussion über die zu leichte Zerstörbarkeit der MX-Raketen in den USA und der Entscheidung der Reagan-Administration, 100 MX-Raketen in bestehenden Minuteman-Silos zu stationieren [27], wurden der Verteidigungsminister Caspar Weinberger und der Vorsitzende des „Joint Chiefs of Staff“ General John Vessey vor dem „Senate Appropriations Committee“ angehört. Auf den Vorwurf, daß die MX-Raketen in diesen Silos zu verwundbar seien, antworteten beide, daß dies nur der Fall sei „if we ride out the attack“, d.h. nur dann seien sie verwundbar, wenn sie nicht bereits aufgrund der Vorwarnung abgeschossen seien. Auf Befragen der Senatoren sagte General Vessey erneut: „the Soviets have no assurance that we will ride out the attack“, jedoch auf die bohrenden Nachfragen der Senatoren, ob dies bedeute, daß die USA bereits eine „Launch-on-Warning“-Strategie übernommen habe, verweigerten Weinberger und Vessey die Aussage [23].

„Launch-on-Warning“-Vorschläge in der UdSSR

Die Sowjetunion hat vor der Stationierung der Pershing-II-Raketen mehrfach angekündigt, sie werde die Bedrohung durch diese Raketen als so schwerwiegend ansehen, daß sie nach deren Stationierung eine „Launch-on-Warning“-Strategie verfolgen werde. Diese Ankündigung wurde u.a. in der Washington Post vom 11. April 1982 nachgedruckt: In dem Artikel wurden offizielle Angaben der Sowjetunion zitiert, nach denen der Abschub der Raketen weitgehend vollautomatisch durch Computer vollzogen und jede menschliche Eingriffsmöglichkeit abgeschafft werden solle.

In einem Artikel der Prawda vom 12. Juli 1982 hat der Verteidigungsminister Dimitri Ustinov den Übergang zur „Launch-on-Warning“-Strategie angedroht, und in einem Buch von A. Cox [9] wird G. Arbatov, Mit-

glied des sowjetischen Zentralkomitees, mit dem gleichen Vorschlag zitiert. Der Präsident der sowjetischen Akademie der Wissenschaften, Anatoly Alexandrow, hat einen ähnlichen Vorschlag geäußert [31].

In [20] analysiert der amerikanische General D. Graham die sowjetische Militärstrategie und kommt zu dem Schluß, daß die Sowjetunion zu einer „Launch-on-Warning“-Strategie übergegangen sei.

In einer Stellungnahme im März 1983 [19] hat Ustinov jedoch erklärt, daß die Sowjetunion keine „Launch-on-Warning“-Strategie annehmen würde.

Ebenso betonte der deutsche Verteidigungsminister Wörner mehrfach, nach wie vor gelte für die NATO die „Launch-on-Impact“-Strategie.

Zusammenfassend läßt sich sagen, daß der gegenwärtige Stand der akzeptierten Militärstrategie unklar ist und es nicht zuletzt wegen der militärischen Geheimhaltung und der Propagandafolgen auch kaum eine verbindliche Aussage geben wird. Sicher ist jedoch, daß bei einer Alarmmeldung, die in der verfügbaren Zeit als echt bewertet wird und eine genügend große Bedrohung darstellt, ein Konferenzverfahren, wie in Abschnitt 5 beschrieben, eingeleitet wird. Kommt es hierbei zur „Missile Attack Conference“ (Alarmstufe 3), die auch die Einbeziehung des Präsidenten vorschreibt, dann entscheiden die Konferenzteilnehmer über die Reaktion auf die Bedrohung. Sofern die Konferenzteilnehmer und insbesondere der Präsident (der Generalsekretär, entsprechende militärische Entscheidungsprozesse in der UdSSR vorausgesetzt) in dieser Konferenz eine tatsächliche Entscheidungskompetenz haben, kann weder ein strenges „Launch on Warning“ mit der Bedeutung eines unmittelbaren Gegenschlages noch ein strenges „Launch on Impact“ mit der Bedeutung, keinen Gegenschlag vor einem gegnerischen Einschlag auszuführen, zwingend sein. Vielmehr wird die Entscheidung von der gegebenen Situation abhängen, also beispielsweise davon, inwieweit eine politische Krisensituation vorliegt, wie stark die Bedrohung ist, in welcher Verfassung die Konferenzteilnehmer sind usw. Wegen der Kürze der zur Verfügung stehenden Zeit wird es Entscheidungstabellen geben, die in Abhängigkeit von einer gegebenen Situation den Konferenzteilnehmern Orientierungen durch weitgehend vorkonstruierte Entscheidungen geben.

Je größer die Bedrohung bei einer Alarmmeldung ist und je mehr die Zweitschlagfähigkeit gefährdet ist, desto größer wird die Bereitschaft sein, einen Gegenschlag bereits auf der Basis der FWES-Raketenwarnung anzuordnen. Eine Gefährdung der Zweitschlagfähigkeit wird sich auch zu Ungunsten der „Launch-on-Impact“-Strategie in den Entscheidungstabellen niederschlagen. In diesem Sinne dürften heute bereits beide Großmächte von einer reinen „Launch-on-Impact“-Strategie abgerückt sein [5].

8. Künftige Entwicklung

Die in den vorigen Abschnitten geschilderte militärische Situation der gegenseitigen Bedrohung hängt weitgehend von dem zuverlässigen Arbeiten von Computern ab und entwickelt eine Eigendynamik, die auf eine immer stärkere Integration der Informationstechnologie in die Waffenentwicklung hinausläuft. Für diesen Typ der Kriegführung – „the computerized battlefield“ – wird die *Informatik* zur waffentechnisch *entscheidenden Grundlagenwissenschaft*, so wie es die Physik in der Entwicklung der A- und H-Waffen und deren Trägern war und die Chemie für die chemischen Waffen.

Neben der Entwicklung von Strahlenwaffen und der Militarisierung des Weltalls, die hier nicht näher behandelt werden können, stehen zwei Bereiche im Vordergrund der gegenwärtigen Militärforschung:

- die computergestützte Automatisierung militärischer Entscheidungsprozesse,
- die Entwicklung von Waffen mit (beschränkter) „künstlicher Intelligenz“.

Beispiele für den letzten Bereich sind die selbsttätig ihr Ziel suchenden Pershing-II-Raketen und die Cruise Missiles. Dies ist jedoch nur der Anfang einer Waffentechnologie, die über Fernseh-, Ultraschall-, Infrarot- oder Radarkameras den für sie relevanten Ausschnitt der Umwelt erkennen und über einen Bordcomputer entsprechend gesteuert werden können. Damit sind Raketen möglich, die beispielsweise einen bestimmten Panzertyp erkennen und an dessen verwundbarster Stelle einschlagen oder einen Flugzeugträger an einer genau definierten Stelle treffen können. Raketen, die einen Flugkörper aufgrund seiner Hitzeemission verfolgen (und daher getäuscht werden können), sind durch Raketen ersetzbar, die das für sie vorprogrammierte Ziel ‚erkennen‘ und dann sehr viel genauer verfolgen können.

Die neuen technischen Möglichkeiten werden jedoch nicht nur eine „Verbesserung“ herkömmlicher Waffen bringen, sondern auch völlig neue Waffenarten, vom computergesteuerten Panzer über automatisch gesteuerte Flugzeuge hin zu Kriegerobotern, hervorbringen, deren Erforschung und Entwicklung derzeit im Rahmen des DARPA-Programms gefördert wird [1, 10].

Der zuerst genannte Bereich der Automatisierung militärischer Entscheidungsprozesse wird ebenfalls zunehmend durch Forschungsergebnisse der jungen Wissenschaft „künstliche Intelligenz“ (Artificial Intelligence) geprägt: Beispielsweise ist die Steuerung eines Flugzeugträgers während eines Angriffs von so vielen Einflußgrößen abhängig, daß Menschen durch die Komplexität der Informationsverarbeitung überfordert sind. Ebenso müssen die Entscheidungen zur Steuerung eines Jagdflugzeuges beispielsweise in einer Nahkampfsituation in einer das menschliche Gehirn überfordernden Zeitspanne (Bruchteile von Sekunden) getroffen werden. Die Automatisierung dieser Steuerent-

scheidungen ist daher einer der Schwerpunkte des militärischen Forschungsprogramms DARPA [10].

Dies ist jedoch ebenfalls nur der Anfang einer absehbaren Entwicklung: Militärische Expertensysteme [10] werden zunehmend Einsatzpläne erarbeiten und auch konkrete Einsatzbefehle geben, um die militärische Führung von der immer komplexer werdenden, den Menschen überfordernden Informationsverarbeitung, die in immer kürzeren Zeitspannen zu bewerkstelligen ist, zu entlasten.

Die Entwicklung dieser Technologie wird zu einer immer weiter gehenden *Automatisierung der FWES* führen, die es erlaubt, das derzeit „fehleranfälligste Element“ in den FWES – den Menschen – weitgehend durch Computer zu ersetzen.

Das amerikanische Verteidigungsministerium hat im Rahmen des DARPA-Projektes allein für die Erforschung dieser neuen Techniken 1 500 000 000,- DM für einen Zeitraum von fünf Jahren zur Verfügung gestellt.

9. Schlußbemerkung

Die Gefahr, daß isoliert auftretende Fehler in einem FWES in Friedenszeiten zu einem Atomkrieg führen, ist bei den vorhandenen Sicherungssystemen relativ gering. Doch wenn

- eine politische Krisen- oder Konfliktsituation vorliegt,

- mehrere Ereignisse gleichzeitig eintreten,

- Alarmierungsketten initiiert werden und

- die Zweitschlagfähigkeit gefährdet ist,

dann ist die Gefahr von Fehlern und Fehleinschätzungen, die zur Auslösung eines Atomkriegs führen können, nicht auszuschließen, sie kann situationsabhängig sogar drastisch ansteigen.

Die in der Einleitung erwähnten Sicherheitsmaßnahmen gegen einen „Atomkrieg aus Versehen“ werden dabei weitgehend hinfällig:

- Im technischen Bereich ist nicht das Versagen einer einzelnen Rakete das Hauptproblem, sondern das Versagen eines Computers. Es ist prinzipiell nicht möglich, solche Fehler auszuschließen.

- Innerhalb der wenigen bei einem Alarmfall verbleibenden Minuten kann kein sinnvoller Ost-West-Dialog über den „heißen Draht“ aufgebaut werden.

- Mit immer raffinierteren technischen Verfahren, die beispielsweise die Treffsicherheit nuklearer Raketen erhöhen, wird die Zweitschlagfähigkeit gefährdet. Um trotzdem eine glaubwürdige Abschreckung aufrecht zu erhalten, wird ein Übergang zur „Launch-on-Warning“-Strategie nötig.

Der gesamte technologische und militärpolitische Prozeß läuft auf eine immer stärkere „Kopplung“ der Waffen- und Informationssysteme beider Weltmächte zu *einem einzigen System* hinaus, in dem auf technischer Ebene Interaktionen auftreten können, die nicht vorhersehbar sind und von Menschen nicht mehr kontrol-

liert und beherrscht werden. Diese Entwicklung verläuft unter dem Druck der technischen Möglichkeiten sehr schnell, und es ist äußerst fraglich, ob es überhaupt noch möglich ist, sie aufzuhalten.

Insbesondere wir Naturwissenschaftler, aber auch die Politiker müssen erkennen, daß diese Entwicklung allein mit technischen Mitteln nicht beherrscht oder gestoppt werden kann, sondern nur durch ein politisches Umdenken.

Politische Konflikte können durch einen Nuklearkrieg nicht mehr ausgetragen werden, und damit ist bei weitem nicht alles, was technisch machbar wäre, unter dieser Einsicht auch politisch sinnvoll. Die Frage ist, ob das führungslos galoppierende Pferd technologischer Entwicklung durch politische Einsicht gezähmt werden kann und politische Maßnahmen wieder zum Primat – nicht zur bloßen Folge – militärtechnischer Entwicklungen werden.

Liste der Abkürzungen

ANMCC	Alternate National Military Command Center
BMWES	Ballistic Missile Early Warning System
CSS	Communication System Segment
EMP	Elektromagnetischer Puls
FWES	Frühwarn- und Entscheidungssystem
ICBM	Intercontinental Ballistic Missile
JCS	Joint Chief of Staff
NCS	NORAD Computer System
NMCC	National Military Command Center
NORAD	North American Aerospace Defense Command Center
PAC	Pacific Command
PARCS	Perimeter Acquisition Radar Attack Characterization System
SAC	Strategic Air Command
SCC	Space Computational Center
SLBM	Submarine-launched Ballistic Missiles
WWMCCS	World Wide Military Command and Control System

Dieser Artikel ist eine überarbeitete Version von [28] und [7]. Wir danken unseren Kollegen H. J. Bürkert, N. Eisinger, A. Herold, C. Lingenfelder, H. J. Ohlbach, W. Olthoff und C. Reddig-Siekmann für die konstruktive Kritik in zahlreichen Diskussionen sowie für die vielen Hinweise bei der Vorbereitung dieses Artikels. Wir danken außerdem Prof. K. Haefner, Universität Bremen, durch dessen Engagement in zahllosen Diskussionen, Vorträgen und schließlich in einer gemeinschaftlichen Verfassungsbeschwerde die hier dargestellte Problematik im deutschsprachigen Raum erstmalig bekannt wurde. Durch Alan Borning, CPSR, haben wir Zugang zu vielen amerikanischen Veröffentlichungen und Informationsmaterial bekommen.

Literatur

1. Barlow, K. A.: Konzepte für den Einsatz von Robotern mit künstlicher Intelligenz. Direktorium, Institut for Strategic Studies, 1983
2. Betts, R.: Soldiers, Statesmen and Cold War Crisis. Cambridge Mass. 1977
3. Boeker, E.: Der Erstschat wird möglich, in: Naturwissenschaftler gegen Atomrüstung, SPIEGEL-Buch 45, Rowohlt 1983
4. Borning, A.: Computer System Reliability and Nuclear War. Department of Computer Science, FR-35, University of Washington, Seattle, Washington 98195, July 1984

5. Bracken, P.: The Command and Control of Nuclear Forces. New Haven: Yale Univ. Press 1983
6. Bitdorf, W., Sampson, A.: Sinken auf eins-null-tausend . . . SPIEGEL-Serie, Beginn No.39, 1984
7. Bläsius, K. H., Siekmann, J.: Computergestützte Frühwarn- und Entscheidungssysteme, in: Wissenschaft und Rüstung (Bähren, H., Tatz, J., Hrsg.). Steinweg-Verlag 1985
8. Clarius, F.: Frühwarn- und Entscheidungssysteme. Universität Kaiserslautern 1985, interner Bericht
9. Cox, A. M.: Russian Roulette, the Superpower Game. New York: Times Book 1982
10. DARPA: Defense Advanced Research Projects Agency, Strategic Computing Proposal, October 1983
11. Dumas, L. J.: Human Fallibility and Weapons. Bulletin of the Atomic Scientists 36 (9), 15 (1980)
12. Easterbrook, G.: Try an MZ Missile. New York Times, 18. Februar 1983
13. McElheny, V. K.: Improbable Strikes by Lightning tripped its System, Con Ed Says. New York Times, 15. Juli 1977
14. Finer, H.: Dulles over Suez. Chicago Quadrouple, p.418, 1964
15. Federal Power Commission: North Eastern Failure: Nov.9 and 10, 1965. Washington D.C.: US Government Printing Office 1965
16. Federal Power Commission: Prevention of Power Failures. Washington D.C.: US Government Printing Office 1967
17. Garwin, R.: Launch under Attack to Redress Minuteman Vulnerability? International Security 4 (3), 1979
18. US General Accounting Office: NORAD's Missile Warning System: What went wrong? MASAD-81-30, May 1981
19. Gelb, L. H.: Soviet Marshal warns the U.S. on its Missiles. New York Times, 17. März 1983
20. Graham, D. O.: Shall America be Defended? New Rochelle, New York, p. 87 und p.257, 1979
21. Haefner, K., et al.: Verfassungsklage gegen den Betrieb von Frühwarn- und Entscheidungssystemen. Nachgedruckt u. a. in Frankfurter Rundschau
22. Hart, G., Goldwater, B.: Recent False Alerts from the Nation's Missile Attack Warning System. United States Senate, Committee on Armed Service, Washington D. C. 1980
23. Halloran, R.: Shift of Strategy on Missile Attack Hinted by Weinberger and Vessey. New York Times, 6. Mai 1983
24. International Institute for Strategic Studies: The Military Balance 1983-1984. London: IISS 1984
25. Kreck, M.: Eine ganz neue Entwicklung: Vergleich der Erstschlagfähigkeit von Pershing-II und SS-20 aus mathematischer Sicht, in: Naturwissenschaftler gegen Atomrüstung, SPIEGEL-Buch 45, Rowohlt 1983
26. Rogovin, M., Frampton, G. T.: Three Mile Island, a Report to the Commissioners and to the Public. Nuclear Regulatory Commission Special Inquiry Group, U.S. Nuclear Regulatory Commission, Washington D.C. 1980
27. Scowcroft, B.: Report of the President's Commission on Strategic Forces. U.S. Dep. of Defense 1983
28. Siekmann, J.: Computergestützte Frühwarn- und Entscheidungssysteme, in: Nachdenken statt Nachrüsten (Buckel et al., Hrsg.) von Loeper Verlag 1983
29. Sorensen, TH. C.: Kennedy, p.577. New York: Harper and Row 1965
30. Steinbrunner, J.: Vergeltungsschlag bei nuklearem Angriff (Launch under Attack). Spektrum der Wissenschaft, März 1984
31. Washington Post: Soviet Warns of Automatic Retaliation Against new U.S. Missiles. 18. Mai 1983

K. H. Bläsius, J. H. Siekmann
 Universität Kaiserslautern
 Fachbereich Informatik
 Postfach 3049
 D-6750 Kaiserslautern