# The Impact of Federal German Intelligence Service Bundesnachrichtendienst (BND) Project RAHAB and Chaos Computing Congresses (CCC) impact on the Future of Computer-Network Mediated Espionage: Cuckoo's Egg Prequel or Perfect Storm?

# The Impact of Federal German Intelligence Service Bundesnachrichtendienst (BND) Project RAHAB and Chaos Computing Congresses (CCC) impact on the Future of Computer-Network Mediated Espionage: Cuckoo's Egg Prequel or Perfect Storm?

## ABSTRACT

The Cuckoo' Egg Investigation – a term coined by American press to describe (at the time) the farthest reaching computer-mediated espionage penetration by foreign agents, was also known as Operation EQUALIZER initiated and executed by the KGB through a small cadre of German hackers. Although the details of the investigation pour out page after page in Cliff Stoll's first-person account titled *The Cuckoo's Egg*, few asked and sought to understand, "Where did the CUCKOO'S EGG hackers come from? What were the conditions that made the CUCKOO'S EGG penetrations a reality? Did the CUCKOO'S EGG penetrations exist in isolation to other events – was it a one-off?" The following historical research uses the evolution of a 1981-1991 West German Intelligence Agency (BND) computer-mediated espionage effort named Project RAHAB as a basis for analysis of competing hypothesis (ACH) to answer what came before the CUCKOO'S EGG penetrations and how the events relate. Project RAHAB serves as a lens to interpret the growth and maturation of computer-mediated economic and technological intelligence capabilities of other state sponsored intelligence agencies during the 1980's, as well as represent a means to examine precursor events leading up to the CUCKOO'S EGG penetrations and subsequent investigations.

## INTRODUCTION

> "Cyber war is like Carl Sandburg's fog; it comes on little cat feet, and it's hardly noticed. That's its greatest potential."
>
> John Arquilla,
> Associate Professor of Defense Analysis
> Naval Post-Graduate School
> (PBS Frontline Public Broadcast Transcript,
> April 24th, 2003).

In December 1969, the Advanced Research Projects Agency Network (ARPANET) took the first step toward interconnecting computers into a network for general communications. Over the next decade, ARPANET grew from 4 nodes to 113 interconnecting academic, defense contractor, and armed services branch network nodes. In 1983, the Military nodes of ARPANET broke off to form a separate network known as the Defense Data Network (MILNET). MILNET, an abbreviation for Military Network, contained 68 network nodes and ARPANET retained 45 network nodes. Although the networks were separated, the internetwork design did not mandate full compartmentalization. The national laboratories, founding academic universities, and defense contractors, remain inter-connected to MILNET. ARPANET and MILNET network access was bi-directional. Over time European networks could reach ARPANET. During the midpoint of the 1980's, ARPANET eventually matured into NSFnet, which morphed into the Internet. MILNET matured into two compartmentalized networks known as the Secret [formerly Secure] Internet Protocol Router Network for classified information (SIPRNet), and the Non-classified Internet Protocol Router Network (NIPRNet). NIPRNet is used to exchange unclassified but sensitive information between government entities and provide Internet access (Atlas of Cyberspace, 2004).

Computer networking concepts are distinctly American. In 1958, the Eisenhower Administration formed the Advanced Research Projects Agency (ARPA). By 1966, ARPA was laying the foundation for general purpose network communication. America prides itself as an open society; ARPANET reflects the values of collegiality, openness, and growth. By 1985, ARPANET evolved into its' second generation, known as NSFnet. America was far ahead of the rest of the world in networking. The full expanse of ARPANET could not be reached by Germanic research institutions until after the West German National Telephone Service (Bundespost) launched Data Network Services (DATEX-P) in 1985. DATEX-P was able to reach ARPANET through TYMNET International Gateway Routing Service via either a satellite link or transatlantic cable. The same openness and collegiality that made ARPANET a success, was also its' major weakness.

In 1985 The German Federal Intelligence Service, known as the Bundesnachrichtendienst (BND), under the Directorship of Eberhard Blum, showed increasing interest in computer networking. The BND expressed a desire to explore the extent to which network access can provide venues for espionage and foreign intelligence collection. The BND performed field observation of West German hackers, specifically a group formed in 1981 called the Chaos Computer Club (CCC)[1]. In the fall of 1984, CCC members, with assistance from another group called VAXBusters[2] based out of Heidelberg, penetrated the Bildschmirmtext (BTX) Computer Network and successfully debited the Hamburger Sparkasse saving bank account for DM134, 000.00 and credited a

[1] The CCC in 1984 and 1985 was small. As derived from the Mungo and Clough's personal interviews with core CCC members at the time, the census was about 150 members (Mungo and Clough 172, 1992).
[2] The VAXBusters were a group of hackers whose goal was to defeat VAX security and penetrate all VAX systems internationally (Mungo and Clough 80, 1992).

CCC account. The CCC returned the money the following day during a staged public event designed to demonstrate their abilities. From 1981 to 1988, Christian Stoessel, a BND field officer, identified the CCC as a collection target, and began observing and recording the CCC's maturing capabilities and personalities – by extension also those who later formed the VAX buster's hacker group, and Hannover (Cuckoo's Egg) hacker group.

In 1987-1988, Stoessel built upon Blum's interest in computer espionage by publishing an internal BND operational proposal promoting the merits of computer network access, computer hacking, software viruses, and the value such activities would bring to the BND. In 1988, Stoessel formally created Project RAHAB[3] as a hybrid effort between BND Division I Human Intelligence (HUMINT), BND Division II Signals Intelligence (SIGINT), and BND Division IV Headquarters (HQ). Specialist from other armed services intelligence branches, law enforcement agencies, domestic counter-intelligence agencies, and outside private research institutions were added to the project. The stated goal of Project RAHAB alledges to uncover, develop, and maintain systematic covert BND pathways to foreign computer networks, computers, and databases (Schweizer 160, 1993).

Other state sponsored intelligence organizations such as Israeli Mossad, French Directorate Generale de la Secutité Exterieure (DGSE), and Soviet Komitet Gosudarstvenoi Bezopasnosti (KGB), also known as the Soviet Committee for State

[3] Rahab was a prostitute who hid and protected two spies sent to Jericho by Joshua, an Israelite prophet (God's Commission to Joshua 1:1-11). Rahab protected them in exchange for their protection, once Jericho was destroyed (2:1-24). On a historical note, Rahab was able to conceal Joshua's spies despite the King of Jericho knowing where and when the spies arrived. Rahab was able to send the King's loyalists on a wild chase. Internet. Found in "Joshua: The Conquest of Canaan." Located at University of Cumberland http://religion.ucumberland.edu/hebrewbible/hbnotes/joshuanotes.htm. Accessed on 5 April 2007.

Security, were very active in economic and technological intelligence using traditional methods. However, the BND allegedly decided to pursue penetration of foreign computing assets as means acquire intelligence abroad. Clearly the ability to execute espionage from a stand-off distance, use covert approaches with excellent concealment opportunities, and the quick sorting and retrieval of information and data is attractive; it's the same model that fuels modern multi-billion dollar international computer crime.

Project RAHAB is a unique case worthy of study, specifically in contrast to its' target collection activities directed at the CCC, and the events proximal to the CUCKOO'S EGG investigation. The BND's goals for Project RAHAB, and the operational outcomes, may be used as a lens to interpret the growth and maturation of computer-mediated economic and technological intelligence capabilities of other state sponsored intelligence agencies during the time period, as well as represent a means to examine precursor events leading up to the CUCKOO'S EGG penetrations and subsequent investigations. Was Project RAHAB's success the hallmark historical event upon which other Intelligence services realized that penetration and infiltration of foreign networks, computers, and databases is as important as traditional intelligence methods? Did Project RAHAB serve as a prequel exemplar for Operation EQUALIZER (a.k.a The Cuckoo's Egg)?

## RESEARCH OBJECTIVES

Four hypotheses derived from competitive analysis are put to use to examine unclassified information regarding the historical context, development, evolution, deployment, operation, and outcomes Project RAHAB. An analysis of the West German historical context relating to computing and espionage during 1981 through 1991, serves

as a basis for the competitive analysis. The research effort discusses RAHAB in context with major foreign intelligence service computer-mediated espionage penetrations, namely the 1985-1987 Cuckoos Egg Investigation (a.k.a KGB Operation EQUALIZER), other noteworthy computer virus attacks, and overall technology development during the time period.

> Hypothesis 1 (H1) – BND Project RAHAB was not a real computer-mediated foreign intelligence espionage program.
>
> Hypothesis 2 (H2) - The BND was the first state-sponsored intelligence service to fund and formalize systematic computer network penetration of foreign computing assets for the purposes of espionage.
>
> Hypothesis 3 (H3) - Project RAHAB was not the hallmark state sponsored computer-mediated espionage program between 1985 and 1991.
>
> Hypothesis 4 (H4) - Project RAHAB served as the incubator for networked UNIX and VMS computer science critical mass necessary to make Operation EQAULIZER (the Cuckoo's Egg penetrations) a reality.

## REVIEW OF THE LITERATURE

### Concession and Defeat

The West German Intelligence Service has slowly grew in capacity out of concession and defeat. During the decade of 1980, the cultural strain, suspicion, dissention, treason, and defection observed in West German society mirrored in the intelligence services. West Germany enjoyed wide ranging international contacts, modern infrastructure, and close collaboration with North American Treaty Organization (NATO) allies; yet struggled against the infiltrations and undue performance distortions created by damaging KGB, Intelligence Directorate of the Soviet General Staff (GRU) and Soviet Bloc surrogate agency intelligence operations against West German internal security. Judging according to 1980 standards, the West German intelligence apparatus is

one of the larger and foremost allied intelligence services. Unlike the geographic proximity of the U.S. Intelligence agencies, the West German Intelligence Services are decentralized and dispersed (Polgar 80, 1987). In a country where the culturally ingrained Teutonic orderliness even coalesce anarchists into groups with designated meeting locations, The 1987-1988 RAHAB operation stands unique. The project was a cross-organizational matrix organization which included members of BND Division I (operational procurement and HUMINT), BND Division II (technical intelligence), BND Division IV (administration), Amt für Fernmeldwesen Bundeswehr (German Defense Ministry Radio Monitoring), Amt für Nachrichtenwesen Bundeswehr (Federal Armed Forces Intelligence Office), Bundessamt für Verfassungsschutz (German domestic secret service, state security, and counter-espionage – a.k.a BfV), plus select members of academic institutions, government research outlets, and private companies (Schweizer 160, 1993). BfV personnel and BND agents worked closely. The Bundespost (German Post Office) played a critical, but unstated role. The Bundespost was responsible for State accounting and administration of mailboxes, telephones, dial modems, and granting access into the German National Telephone System; ultimately being the lone agency tracing down the first Cuckoo's Egg Hacker, Marcus Hess. Operation RAHAB was based out the Frankfurt Institute of Social Research; a location removed from its' primary collection target, the Chaos Computer Club (CCC), based out of Hamburg. The CCC was formed in 1981 by a computer hobbyist and democratic socialist named Wau Holland. The CCC was a collection of computer academics, students, lock pick specialists, futurists, anarchists, and computer programmers who viewed technology as an equalizer and a force for social change (Mungo and Clough 79-80, 1992). In 1981, BND Field

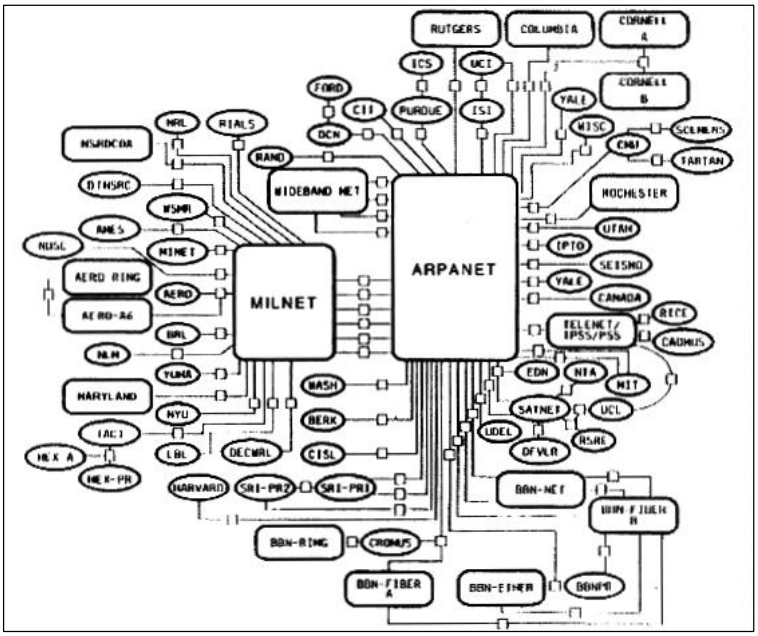
Officer Christian Stoessel identified the CCC as a collection target, and observed and recorded the CCC's maturing capabilities and key personalities. By 1984, West Germany was on par with the U.S. for the number of accomplished hackers and equivalent in operational daring. During the 1980's, West German hackers would be affiliated with high-profile network penetrations internationally for the next six years (Mungo and Clough 172, 1992). Appendix A and B provide a chronological timelines paralleling BND RAHAB, CCC, Early Computer Virus Development, and Cuckoo's Egg key events during the eight year period.

From 1981 to 1984, private computing, academic computing, computer programming, and computer networking developed critical international mass. By 1985, U.S. and European academic and classified networks were a dense web of ubiquitous and homogenous interconnections. Thirty-Two individual national or scientific networks joined to form a massive international internetwork (Madsen 414, 1993). In 1983, ARPANET network nodes were split off from MILNET nodes. However, whether the partition is an administrative accounting measure or a true split is contested as evidence by *Diagram 1: ARPANET and MILNET circa 1983* (refer to Appendix C for a network topology map of MILNET (DDN) circa 1989 for further understanding of the global reach of MILNET). It is important to note that during the decade of 1980, International Business Machine (IBM) model 360/370 and Digital Equipment Corporation (DEC) UNIX and VAX VMS[4] computers are the dominant international computing platforms in government, military, and academic high-performance computing. IBM and DEC

[4] VAX VMS – Virtual Address Extension Virtual Memory System. The computing system provided true multi-user, multi-tasking, and virtual memory operations. VAX VMS and the IBM model 360 and 370 mainframe computers were competing software and hardware platforms.

homogeneity dominated the NATO computing landscape as the status quo. The personal computer was not present in large numbers during the first half of the 1980's.

Diagram 1: ARAPNET and MILNET Circa 1983-1984




Atlas of Cyber Space (2004). *Historical maps of Computer Networks*. Internet. Found at http://www.cybergeography.org/atlas/historical.html. Accessed on 18 January 2007.

## RAHAB and the CUCKOO'S EGG: Critical Mass in Historical Context

1985 to 1986 is the pivotal time period in West German hacking and computer-mediated espionage history. The Second CCC Congress (1985) and Third CCC Congress and Virus Forum I (1986) are major convergence points. In 1985, The Heidelberg VAX Buster group attended, as well as Karl Koch, future member of the Hannover Hackers[5].

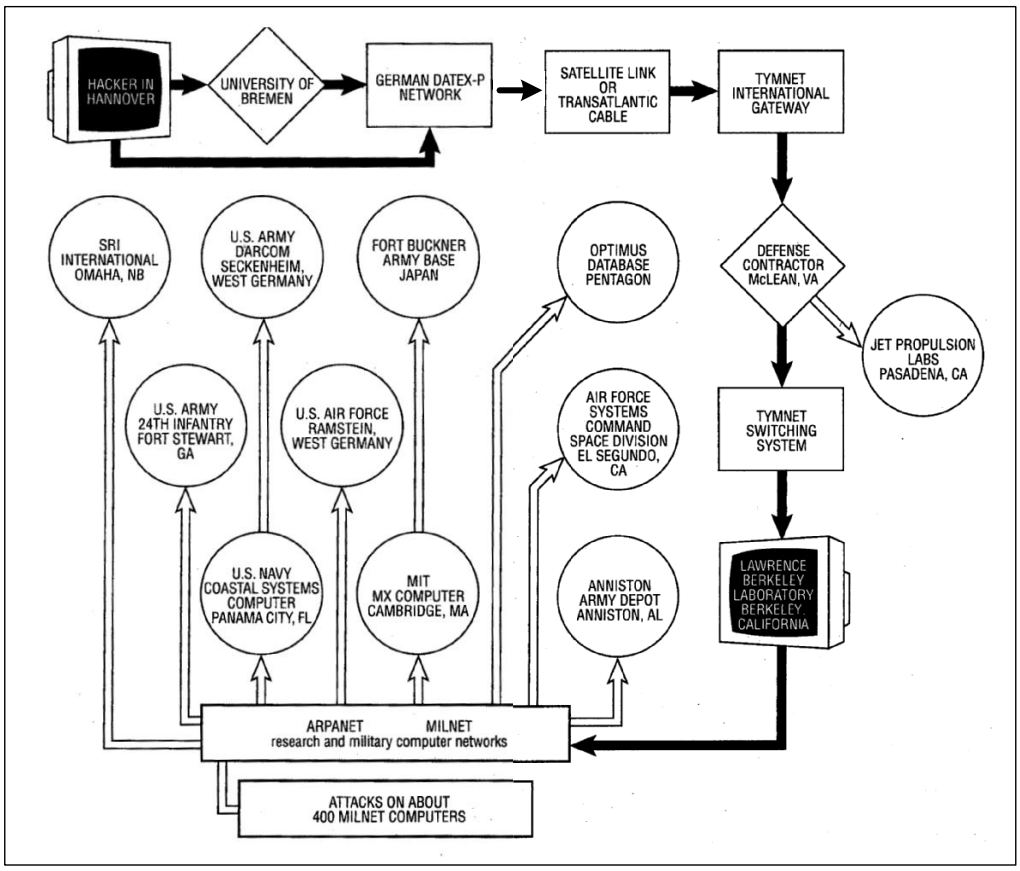
[5] The KGB sponsored hackers were Karl Koch (Hagbard), Hans Huebner (Pengo), Peter Kahl, Dirk Brescinsky, Markus Hess, and Laszlo Balough, a Middle East arms dealer located in Pittsburgh, PA with contacts inside the Bulgarian Intelligence Service (Stoll 256-260, 1989; Madsen 414, 1992). KGB pressure forced Koch into attending the 1985 Congress to seek out other VAX hackers; it is how he came in contact with the Hans Huebner and the VAX Buster group (Mungo and Clough 174 - 179, 1992). See the chronological timeline located in Appendix B for how the CCC, VAXBusters, and the Hannover Hackers related to each other.

who, plus others, later became defendants in the CUCKOO'S EGG investigation. The KGB named the CUCKOO'S EGG computer espionage effort Operation EQUALIZER. Koch and five others were later arrested by German authorities for KGB sponsored computer espionage against U.S. scientific and military computing installations. KGB recruitment for the operation began in 1985, in Berlin (Madsen 418, 1993). The U.S. press reported the outcome of EQUALIZER as the CUCKOOS EGG. In Cliff Stoll's own attempt to humor himself during his search for the source of a 75 cent accounting error, in his book *The Cuckoo's Egg* he established a sting operation called SHOWERHEAD which hosted a bait project named SDINET. KGB Hannover hacker Marcus Hess downloaded the bait June 1987 while hacking into Lawrence Berkeley National Laboratory (LBNL), bait which was then used in his subsequent arrest (256-267). In 1986, Ralf Burger, a computer programmer from Bremen, demonstrated the first working self-replicating native file modifying IBM Personal Computer (PC) Desktop Operating System (DOS) virus named *"Virdem."* Bernd Fix, a student from Heidelberg University, demonstrated the first working IBM model 360/370 mainframe virus known as the "*Fix virus.*" DEC UNIX and VAX VMS computer enthusiasts where in the majority at the Third Congress, plus and anyone else who wished to pay the entrance fee.

In 1985, the Bundespost put the DATEX-P data network into production. The West German national telephone and data network was now tied into all other nation state computer networks through the TYMNET International Gateway via satellite link or undersea trans-Atlantic cable. As uncovered and made public during the 1986 CUCKOOS EGG penetration, the KGB sponsored Hannover Hackers entered into U.S. networks through the TYMNET international gateway to a private business defense

contracting corporation in McLean Virginia (MITRE), were able to transit through LBNL networks, then successfully and repeatedly reach MILNET and ARPANET. The CUCKOO'S EGG investigation revealed that four-hundred U.S. servers were attacked. *Diagram Two* is a visual depiction of the route taken by the KGB-funded Hannover Hackers.

Diagram 2: High-Level Network Topology of the KGB Sponsored Hannover Hackers Penetration of Lawrence Berkley National Laboratory, ARPANET, JPL, and MILNET




Stoll, Cliff (2000). *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. NY: Pocket Books. p. 2

**Vulnerability, Uncertainty, Complexity, Ambiguity**

During the 1985 to 1988 time period, internal West German state security showed its' fragility. A high-value West German intelligence target named Richard Mueller was in hiding inside West Germany. Mueller was sought by the U.S and West Germany for illegal export of COCOM-controlled [6] computers almost exclusively to Soviet trade officials; some of which were KGB or GRU undercover intelligence officers. Muller was believed to operate as many as 75 dummy corporations scattered among NATO nations. The amount of illegal export was estimated to be in the millions of dollars. The Mueller exports included COCOM micro-electronics, microprocessors, peripherals, and semiconductor equipment. In 1983, Mueller successfully exported seven large DEC VAX super mini-computers with software and hardware. The VAX acquisitions were in need to further Soviet computer-assisted design (CAD) for microelectronic fabrication. In late 1983, much of the shipment was seized by Sweden and the BND (DTIC Report AD-A160-564: Soviet Acquisition of Militarily Significant Western Technology: An Update 27, 1985).

The summer of 1985 led to the arrested of many West German senior secretaries in key government offices. Manfred Rotsch, 1967 to 1984 West German Head of the Planning Department of the aviation firm Messerschmitt-Bolkow-Blohm (MBB), passed information to KGB handlers regarding the TORNADO air-craft introduced by the European Panavia consortium (DTIC Report AD-A160-564 20, 1985). The summer ended with the defection of the Chief of the East German Branch of the BfV counter-intelligence agency, Hans Jochim Tiedge, who was a 25 year BfV veteran privy to the

[6] The Coordinating Committee (COCOM) was established in 1949 to serve as the forum for Western efforts to develop a system of strategic export controls. COCOM is composed of the United States, Luxembourg, Japan, Italy, Greece, France, Federal Democratic Republic of Germany, Denmark, Canada, and Belgium.

most sensitive state matters. According to Polgar (1987) reports of espionage between the BND, BfV, and KGB, Staatssicherheitsdeinst (STASI) plus other Eastern European Bloc state intelligence programs was excessive by modern standards. In the period of January 1984 to July 1985, the East Germans reported the arrest of 768 West German Agents. The West German numbers are more modest, but comparable (Polgar 92-93, 1987).

According to Madsen (1993), 1983 French *Service de Documentation Exterieure et de Contre-espionage* (SDECE) collection of Soviet documentation from KGB Department T, known as the FARWELL documents, reveal that Soviet computer hacking is involved in 2.4% of all Soviet espionage operations. Madsen also reports that in upwards of 75 West German companies had technology links to the KGB or GRU in violation of the COCOM export control laws (419).

Many other types of advance electronic technology were sought as well, such as advanced circuit design, semi-conductors, micro-processors, avionics, optics, orbiter technology, engine design, peripheral computing, digital storage, encryption are among the targets (DTIC Report AD-A160-564 3, 1985)The KGB and GRU targeted both the IBM model 360/370 and DEC VAX VMS systems for collection[7]. The model 360 and model 370 exist (at the time) as technical cornerstones of NATO missile defense. The Soviet government recognized that in order to cut research and development time off of their own computerized capability; western source code technology must be acquired. The IBM 370 design and code base was used by the Soviets as the model for production

[7] IBM – International Business Machines. IBM Corporate Executives frequently complained that IBM technology is continuously targeted for collection by state-sponsored intelligence operations in France, Japan, USSR, East Germany, and West German intelligence (Schweizer Chapter 1, 1993). To serve as an example, The KGB and GRU ranked IBM 19th out of 100 U.S. companies for targeted espionage activities. *Source*: "Table 3 Rank Ordering of Top 100 Defense Contractors of 1983 Compared with Their Rank Ordering by Approximate Frequency of Soviet Identification for Needed Technology, Selected Periods in Late 1970s and Early 1980's" (DTIC Report AD-A160-564 18, 1985).

of their own version, codename RYAD (also knows as OS EC), which is a copy of the IBM 360/370 architecture and functions. The 360 and 370 systems were high priority targets; they were identified as most critical to producing future weapons systems, namely the military RYAD computing systems. However, the Soviets lacked the skill and experitise for computer-mediated acquisitions and sought to recruit others. Having recruited Hannover hacker Karl Koch earlier, Koch became the vehicle through which the KGB aquired other IBM and DEC vigilante or mercenary talent and capability.

In 1985, under greater pressure from Berlin KGB handlers, Karl Koch traveled to Karlsrhule seeking a DEC VAX VMS hacker named Steffen Weirhruch. Weirhruch provided Koch with a crafted software tool designed to automatically and deeply exploit a dangerous back-door[8] access point in the VAX system. The hidden administrative backdoor was previously discovered by two Heidelberg hackers code-named Bach and Handel.[9] The Weirhruch tool was a password stealer that was covert, selective, and self-concealing. Once installed the tool cloaked its' presence, only recorded the access credentials of privileged system users in a record that could be picked up later, and erased its' activity as recorded in the computing system logs[10]. Koch acquired the tool and sold it to the KGB in exchange for money and drugs. Bach and Handel also came into possession of the tool; the two were protégés of Weirhruch. Bach and Handel's activities were uncovered in 1986 by University of Heidelberg computing staff. The duo was turned over to the BfV. After full confessions, detailed explanations, receipt of a

[8] A backdoor is a programmatic hidden, sometimes self-concealing, unpublished administrative super user entry point into a software program or software package.
[9] Bach and Handel were the type of VAX experts that Koch hoped to find at the 1985 CCC Congress in Hamburg. Koch was not talented enough himself to meet the demands of the KGB. At that time, he enlisted another VAX VMS hacker, Hans Huebner, a.k.a Pengo (Mungo and Clough 181, 1992).
[10] In modern times, Wierhruch's VAX software is known as a rootkit.

complete listing of all systems penetrated and locations, the BfV informed the U.S. CIA and French DGSE. The DGSE disclosed that Phillips-France and SGS-Thompson computing systems are KGB collection targets. The French DGSE mistakenly took Bach and Handel for CCC (They were VAXBuster members). The DGSE conclusion was based on matching attack footprints between VAXbusters and the Hannover Hackers. Koch's KGB team started Phillips-France and SGS-Thompson penetation and collection efforts in 1986. According to Stoll's account timeline, the Hannover hackers were also fully engaged with United States (US) MILNET and ARPANET assets at the same time. In the Fall of 1986, at the prompting of the DGSE and to the detriment of the CCC membership, the BfV detained or questioned many CCC members, searched dwellings, and seized computing equipment and assets. The BfV overlooked the fact that the VAXBusters were not CCC members. German police had rounded up the most notorious group of German hackers without proper cause further aggravating an already suspicious community – misplaced BfV effort fueled and inflamed West German hacker conspiracy theories; further clouding the environment for the BND. The French DGSE did not believe the 1987 German investigative conclusions. The CCC was not involved in the French penetrations (Mungo and Clough 188-189, 1992). Stoll's findings, DGSE findings, CIA awareness, and the BfV actions never crossed paths.

In the midst of the 1986 public UNIX and VMS hacking, a damaging and heretofore anonymously authored virus arose from Vienna, named the *Vienna virus.* The PC-DOS virus had a destructive payload and the ability to quickly propagate. The Vienna

source code was decompiled, reconstructed, and (unfortunately) published[11]. Vienna was a recipe for any future PC-DOS based virus. The Vienna viruses led to many variants. In 1987 on the campus of Clausthal-Zellerfeld south of Hannover, the first Trojan horse[12] malicious software program was written for the IBM 370 computing system. The Trojan program carried a virus that lacked self-termination instructions (a self-destruct sequence); The virus propagated internationally over computer networks. Upon reaching IBM's private European computer networks, IBM's mainframe network halted from processing pressure (Mungo and Clough 82, 1992). It has been alleged, but not proven, that the Bulgarian Intelligence service was operating a clandestine computer virus breeding operation based out of Sofia, Bulgaria. 1989 West German Bundesskriminalamt (BKA) court documents reveal that one of the KGB-sponsored hackers, (likely Koch or Hess), has visited the Bulgarian Cybernetic Institute in Sofia (Madsen 426, 1993). The 1986 Vienna virus was authored anonymously. No person or group has stepped forward to claim authorship. No link to the KGB or BND can be found.

## ANALYSIS AND DISCUSSION

*Hypothesis 1 (H1) – BND Project RAHAB was not a real computer-mediated foreign intelligence espionage program.*

Based upon surrounding facts in the literature, the BND decision to embrace computer-mediated espionage and proceed forward is a logical progression. It is argued that during the 1980's, West Germany is concurrently struggling with internal security

[11] In order for another to re-build a previously built (compiled) computer virus, the virus executable code has to be reversed (decompiled) to learn the actions performed by the computer code. After modifications are performed and tested, the updated code (known as a *variant*) is re-compiled back into executable form.
[12] Trojan horse program ("A Trojan") – A computer executable program that introduces an unhealthy or malicious element in to an otherwise trusted computing system; analogous to the Roman use of a trojan horse to get hoplite soldiers inside the walls of Greek City of Troy.

weaknesses associated with top-level government positions, facing a massive counter-intelligence apparatus (KGB, GRU, and the Eastern Bloc), dealing with a ground swell of regional UNIX and Mainframe hackers, observing successful computer virus writers, recognizing the impact of homogenous computing and network platforms, and grappling with the exposure of being nationally internetworked to all other nation-states. During 1985 and 1986, it is inferred that West German intelligence is feeling the weight of context. Historical context places the BND at the RAHAB decision point and at an intersection with the CUCKOO'S EGG precursor events.

As a basis, but not as a representation of West German geo-political interests, consider a realist justification to economic espionage rendered by Sherman Kent in his 1949 seminal work *Strategic Intelligence for American World Policy*, Princeton University Press.

> "Economic intelligence has to be cognizant of developments of new doctrines, analytical and scientific methods, policies, and developments in other nation states. Examples include tracking the progress, extension, and application of new resource maturation in industry, utilities, or commodities" (1-2).

Presuppose the German BND is able to assemble the intelligence environment; The BND concludes that the CCC, the Virus Forum, the VAXBusters, the academic computing knowledge base, and the DATEX-P computer network are resources that the service can leverage. It is important to point out, that although not an aim or orchestration of Project RAHAB, collectively these facts represent the nest from which the "Cuckoo" roosted. The Bach and Handel confessions to the BfV essentially provided the BND a roadmap to NATO high-performance computing environments. The out-brief

further revealed the expertise in the community at large, expose the BND and BfV to the class of information covertly obtainable, and revealed potential computer-mediated espionage players. Recall that Schwiezer (1993) stated that the BND and BfV were task force members in RAHAB. The DGSE investigation case and the CUCKOO'S EGG investigation further confirm that the international computing environment was homogenous and without internal security; friendly and unfriendly countries essentially possessed the same structural computer and network security computing dilemmas. Add Stoessel's collections and observations of the CCC since 1981, information culled from DGSE and BND sharing agreements regarding KGB activity, and that Stoessel had a proposal ready to go in 1987, puts the BND at the decision point for Project RAHAB. The aggregate post-impact results of VIRDEM, VIENNA, FIX, CHRISTMAS TREE, and CASCADE viruses[13] demonstrated that a substantive offensive computing capability could be created to operationally degrade or render an adversarial computer network useless. The cost is relatively inexpensive; the ability to attack from a stand-off distance very attractive, and very little manpower is required. The ability to manipulate attack timing is favorable and the covert approach opportunities are excellent. Lastly, the BND knew that the Soviets were trying to close the military computing technology gap with the U.S by using original COCOM or clone hardware and software. A window of opportunity exists to develop the capability to infiltrate, degrade, or destroy the Soviet computing capability, as it was being built.

The corresponding realist policy position is based on West Germany's

[13] The CHRISTMAS TREE virus was a Trojan software payload that released an electronic mail virus. The Trojan virus halted IBM's international mainframe networks in two days. (Mungo and Clough 102-103, 1992). CASCADE was a PC-based DOS virus which halted the IBM Belgium Offices 1987 History. Kaspersky's Virus List. Internet. Found at http://www.viruslist.com/en/viruses/encyclopedia?chapter=153311150. Access on 9 April 2007.

acknowledging its' inability to defeat the Soviet military, nor decrease the lethality of Soviet missile inventory. Based upon the historical context of 1985 and 1986, the BND has the means, motive, opportunity, and the resources to assemble methods to decrease the lethality or potentially stop the Soviet weapons technology programs, *and* increase the economic might of West German industry. Building a focal computer-mediated offensive intelligence capability with an offensive information operations subset is not beyond reality. But, like lightening in a bottle, once released into the ether it remains difficult to contain. If West Germany is in possession of such high-caliber computing knowledge and capability, it was not only best for Germany to expand its' sphere of influence in the arena, it was tantamount to balancing the scales against strong institutionalized friends and foes: NATO and the Soviet Bloc. Hypothesis one (H1) asserts that Project RAHAB is fictitious. Hypothesis one is refuted by a preponderance of evidence. The conclusion is that Project RAHAB was real but for reasons not discoverable - appeared to operate in listen-only mode; to assess but not act.

> *Hypothesis 2 (H2) - The BND was the first state-sponsored intelligence service to fund and formalize systematic computer network penetration of foreign computing assets for the purposes of espionage.*

As earlier stated, According to Madsen (1993), 1983 French *Service de Documentation Exterieure et de Contre-espionage* (SDECE) collection of Soviet documentation from KGB Department T, known as the FARWELL documents, reveal that Soviet computer hacking is involved in 2.4% of all Soviet espionage operations. Madsen also reports that in upwards of 75 West German Companies had technology links to the KGB or GRU in violation of the COCOM export control laws (419). As early as 1978, the Soviets were acquiring IBM technology. The KGB motivations appear to be more suited to national intelligence operations and industrial espionage. Aside from the Bulgarian connection to virus writing during the 1987, and a visit to the Bulgarian Cybernetic Institute by one of the Hannover Hackers, malicious software originating out of Bulgarian did not peak until 1991 (Mungo and Clough 110-111, 1992; Madsen 426, 1993). Offensive military information operations was likely not on the horizon, the Soviets lacked the technology, academic knowledge base, and infrastructure to mass produce their own mini-computers, semi-conductors, transistors, electronic subcomponents, and systems. Operation EQUALIZER (the Cuckoo's Egg) appears on face value as cyber-espionage as defined by Adkins (2001).

> "Cyber-Espionage (computer-mediated espionage) is the use of computer hacking in foreign intelligence operations to obtain information or access to foreign computer systems with the intent to commit espionage or have the access to commit state sponsored sabotage when necessary" (p. 26).

As reported in a 1989 New York Times article written by John Markoff, the Hannover Hackers penetrated the computer network of select French military and electronics manufacturers. Phillips-France and SGS-Thompson were known to produce COCOM-restricted gallium arsenide circuit designs. The COCOM technology is used by military designers in electronic warfare applications such as signal interception and radar jamming. The KGB, GRU, and Bloc intelligence services did target commercial and private data bases. However, the information was generally obtained by undercover agents, visiting academics, science students enrolled in VISA programs, information intermediaries, and open sources (Madsen 426, 1993).

Was the KGB more advance in digital tradecraft than the BND? According to a U.S. Counter-intelligence source noted in Schwiezer (1993) "No one [country], in what at that time was the Soviet Bloc really had the sort of computer network that could be entered" (159 para. 5). However, such statement is not entirely consistent with Madsen (1993) report on KGB capabilities. As early as 1978, the Soviet Union Institute for Automated Systems Network (IASNET) was connected to the unclassed U.S. Defense Data Network (later named MILNET) via proxy through the International Institute of Applied Systems Analysis (IIASA) in Laxenburg, Austria. All three were linked by the TYNMET gateway. In a confidential 1981 memo to President Reagan, Austrian Chancellor Bruno Kreisky reported that the link was used for computerized intelligence gathering (Madsen 426, 1993). Whether the gathering was eavesdropping and interception of the communication link or the communications link was used to access or penetrate foreign computing assets is unknown. The Soviets may not have had a native

internal state network analogous to the United States, but not owning a network is not a precondition to hacking into the assets located on another host network.

Hypothesis two (H2) is only partly supported. It is clear from the available literature that the KGB used digital tradecraft as an augmentation strategy to traditional methods of systematic access to foreign computing assets much earlier that the BND. The BND appears not to be the first state-sponsored intelligence service to fund and formalize systematic computer network penetration of foreign computing assets for the purposes of espionage. The BND may have acknowledged the potential opportunities of state-sponsored hacking early in the 1980's, but observations and motivations could be easily overshadowed by West German internal state insecurity matters. The pace, depth, and success of Soviet offensive operations likely dominated the BND and BfV tactical planning. The degree of KGB digital tradecraft formalization can be challenged. The Soviet KGB was building out state computing infrastructure through collection and acquisition. Unlike West Germany at the time, the Soviet academic, scientific, and infrastructure computing base was not fully mature to leverage acquired technologies. It is plausible that certain technology, reverse engineering, and educational development efforts stalled or halted, when additional technology was needed to move forward. Although the BND Project RAHAB appeared to exist in listen-mode, the Hannover hackers presented the KGB with an opportunistic entry into computer-mediated espionage upon which the agency capitalized through the Hannover hackers plus a fluid, and nearly friction-free U.S. network computing environment. The "Cuckoo" left in search of a nest in which to hatch.

*Hypothesis 3 (H3) - Project RAHAB was not the hallmark state sponsored computer-mediated espionage program between 1985 and 1991.*

Although computer-mediated attacks and electronic warfare captures the imagination, the reality is conventional and closer to three primary motivations: military operational support, national intelligence support, and industrial espionage. Computer-mediated or computer-based intelligence operations are more feasible as an effective means of action. Covert observation or collection through open-sources or hacking is an obvious undertaking, either as a primary objective or for other purposes (Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications Awareness Document 20-21, 2000).

Consider the freedom computer-mediated espionage offers to economic intelligence gathering. Proximate access to targeted information is unrequired. Case officer burden is reduced, if not entirely eliminated. The need to iron out logistics, operational security, and communications is diminished. In most cases the traditional case handler activities can be entirely offloaded to automated functions using pre-programmed computational timing, Internet protocol addressing (IP) location, and cryptologic routines. The case handler general housekeeping functions provide an artifact that can be patterned thus detected and disrupted; not so if a logical computer-mediated case management structure is in place. The ratio of collectors to case manager is no longer limited to the number of cases a human can manage, but limited only by the computing power, timing patterns, and programmatic logic. Logical case management can rapid adjust to changes in collection requirements or target multiple objectives concurrently. The risk reduction is obvious. The opportunity for introducing pre-planned

deception is favorable. Targets have little awareness or recognition of digital attacks and computer-mediated collection activity (Brenner and Crescenzi 4, 2006).

Unlike the Soviet computer-mediated espionage efforts like EQUALIZER, some historical evidence suggests that RAHAB was directed at the United States and not the Soviets. According to the findings of Brenner and Crescenzi (2006), intelligence reports point to 1970 as the year the BND was given a mandate to add U.S. internal interests to the BND collection target list. Their conclusions pointed to the fall of the Berlin Wall on November of 1989 and the breakup of the former Soviet Union as the decision point where the BND focused efforts on economic intelligence. "Consequently, the United States became its primary economic intelligence target."(5) Factor in 1989 MILNET node density in Germany (See Appendix C) a refocus toward U.S. computing assets is plausible.

According to Schweizer (1993), the BND took great interest and allegedly replicated the IBM model 370 *Fix virus*. The *Fix virus* was a destructive payload mainframe virus created in 1986, and introduced by Bernd Fix at the 3rd CCC Congress (See Appendix A). According to Schweizer (1993), BND computer scientists built a test network in likeness of potential adversaries and trialed the *Fix virus*, but abandoned the effort. Schweizer ties up the allegation by stating that the "BND found the virus very complex" and "trials were abandoned out of fear that if used against a potential enemy, the virus could lead to Germany being infected too" (160).

The source code for the *Fix virus* is available for review. The author published the source code. The code is straight forward. It is an MVS assembly language sequential top-down job-step program that creates a memory area, loads modules, makes

entries into the MVS job catalog, launches an infection routine as a loadable module, and furthers itself through dynamic memory allocation. The source code is heavily documented with Fix's remarks (Fix source code for the IBM 3090 MVS/370 System, 1987). According to Fix, the University of Heidelberg mainframe was needed only to prove out the concept. Fix made use of the IBM PC-SIG Library, 4th Edition, which was an IBM-PC software collection published in 1986. The disk set #402, was a cross assembler for the IBM 370 Version R1.1. Fix built the entire virus on a 1986 desktop personal computer which in all likelihood was either an IBM 8088 processor with 640 Kilobytes (KB) of Random Access Memory (RAM) or a 1985 IBM PC-XT 286 with 640 KB of RAM (either form factor was a standard personal computer between 1981 and 1986). Code linking and compile time on Fix's development platform, does not easily coincide with the "20 hours of programming to recreate it [the *Fix virus*] from start to stop" as reported by Schweizer (160). A mainframe computer would compile code much quicker, as compared to the compile time on a PC processor.

Bernd Fix denies Schweizer's BND claims and disavows any cooperation, consulting, or collusion with the BND. However, Fix does acknowledge that the virus would run on the Soviet IBM 370 RYAD clones and the Siemens IBM-compatible mainframes with either no modification, or only slight changes. Fix states that he lost control of the virus in 1987 when University of Heidelberg staff turned the virus source code over to IBM for analysis. According to Fix, IBM reported that the virus was fully functional (Fix 1, 2004). Although the motive and the means to use the FIX virus against the Soviets (if needed) is present, but to few facts exist to infer that BND had a true interest in offensive information operations capability.

Other claims made by Schweizer (1993) include four 1989 BND penetrations into U.S. and U.K corporate computer databases. It is asserted that the break-ins are feasibility tests to prove out the validity of hacking as a viable intelligence operation mode. According to Schweizer, the 1989 tests result in full funding of the BND RAHAB project. However in light of the events, the Schweizer statement appears illogical – the BND had full knowledge of potential computer-mediated espionage viability resulting from DGSE disclosures of classified material loss during the 1986 SGS-Thompson penetrations – 4 years prior to 1989. The BND was implicated in a March 1991 penetration of the Society for World International Financial Transactions (SWIFT) Global Network. During 1985 to 1991, the SWIFT network is an X.25 packet switched network anchored by VAX computers. The author does not reveal sources beyond attribution to anonymous U.S. CIA officials. Given that the BND and BfV received several open-sourced intelligence collections and case briefings documenting the current state of computer hacking, how to access foreign computing assets undetected, how to use or build computer viruses, detailed examinations of existing network and computer security flaws and the techniques needed to defeat them, the author's assertion that RAHAB was funded and operational as late as 1989 remains tenuous. The historical record shows the BND sat on a trove of collected operational capability and knowledge. Returning to the realist policy position in hypothesis one, it remains unclear why the BND would choose to not act upon the mature files revealing computer-mediated espionage techniques obtained mid-decade while heightened West German computer hacking activity occurs between 1985 and 1988. A delay is especially odd in light of documented Soviet, French, Japanese, and Israeli computer-based espionage capability in the same time period and

the homogeneity of the international computing environment (Fraumann 303, 1997; Madsen 421, 1993). Numerous authors affirm that BND Project RAHAB was the hallmark state sponsored computer-mediated espionage program which augured state-sponsored hacking as a primary intelligence tool. However, such a conclusion cannot be supported without more direct facts which place high-profile BND sponsored penetrations of foreign assets closer, or prior to 1987. A 1988 experimental start date for RAHAB appears late, or misplaced given the historical context of 1985 and 1986. Hypothesis three is accepted as valid based upon the review and discussion of the literature. RAHAB was not the hallmark computer-mediated espionage program of the 1980's.

> *Hypothesis 4 (H4) - Project RAHAB served as the incubator for networked UNIX and VMS computer science critical mass necessary to make Operation EQAULIZER (the Cuckoo's Egg penetrations) a reality.*

Based upon the available facts during 1981 – 1989 time period, Project RAHAB existed as a passive listening post oriented to a collection management program designed to capture and analyze evolving computer-mediated espionage tactics, techniques, and capabilities. During the 1985-1986 time period, RAHAB appears to exist in "listen only mode," and not deliberately or opportunistically offensively targeting by digital means the CCC, NATO allies, KGB/GRU, and Bloc nation intelligence apparatus beyond the existing traditional technical and foreign intelligence method available at the time. During the 1985-1986 time period, the German Intelligence apparatus remains under intense offensive intelligence pressure from the KGB and Bloc intelligence allies, further complicated by a number of high profile West-to-East defections.

Operations EQUALIZER (the Cuckoo's Egg penetrations) appear as KGB opportunistic offensive intelligence effort against NATO allies and the United States. EQUALIZER may not have materialized without the sudden swell of West German UNIX and VMS computer science critical mass further concentrated by the CCC so near their operational bases in East Germany; and certainly could not function in a sustained way without the rapid convergence of trans-continental interconnected telecommunications gateways. EQUALIZER success found amplification through broad thematic unawareness and complacency of U.S. computer network operators and the agencies charged with protecting U.S. Interests (excluding Cliff Stoll). Hannover hackers Hess, Koch, Kahl, Brescinksy, and Huebner would have not come in contact with each other, as well as the Heidelberg hackers Weirhruch, Bach and Handel without the CCC as a common crossroads. The KGB knew of the CCC, having instructed Koch to recruit others to join EQUALIZER. It is possible that the BND had awareness of the KGB interest in the CCC, but there is no evidence to suggest that BND counter-intelligence actions took place. Given the notice provided by the DGSE following the 1986 SGS-Thompson penetration, in hindsight it should have come into the clear that Koch and Hess could also be actively targeted US holdings for KGB interests at the same time. The Hess-Koch US MILNET and ARPANET activities did not fully begin to unravel until January 7th 1986, when Hess downloaded Stoll's Bait files in sting Operation SHOWERHEAD, what is known as *The Cuckoo's Egg* SDINET Project files. Hess likely passed the documents to his KGB handler, who passed them to a Bloc intelligence intermediary Bulgarian Operative Balough. Balough followed up with a physical letter requesting all SDINET documents to Barb Sherwin at LBNL; thus establishing a hard

link between the LBNL hacking, Hess, and Balough. On June 21st, 1987 the Bundespost successfully traced Hess's last login and download. Later Stoll learned that after the arrest - the evidence moved to Wiesbaden, the home of the BundesKriminalamt (BKA) Forensic Science Institute and the Wiesbaden US Military garrison. (266-267; 323-328; 279-280; 342; 364). The BKA was not a major player in the original setup of RAHAB, and Weisbaden was not Project RHAHB's analytical base, Frankfurt's Institute for Social Research served that purpose. At the conclusion of 1987, although the distance between Wiesbaden and Frankfurt is 61 Km, no evidence exists to tie Project RAHAB in any way to the CUCKOO'S EGG penetrations either as intermediary-enabled BND intelligence operations against the US interests, or as counter-intelligence operations against KGB-sponsored Hannover Hackers Hess and Koch. Between 1984 and 1987, no evidence can be found to indicate that the BND knew of Koch and Hess KGB ties, and no evidence can be found that indicated the BND might have tried to flip the pair into a triple or double agent scenario. In 1986, The French DGSE, CIA, and BfV all failed to connect the dots between the SGS-Thompson penetrations and the LBNL penetrations. Hypothesis 4 has no support. Project RAHAB did not serve as the incubator for networked UNIX and VMS computer science critical mass necessary to make Operation EQAULIZER (the CUCKOO'S EGG penetrations) a reality. RAHAB was not a prequel to, or incubator of, the CUCKOO'S EGG penetrations. The incubator was a confluence of events in West and East Germany in 1985 and 1986.

## CONCLUSION

Project RAHAB was one of several elements leading to a perfect storm involving culturally, socially, technologically, geopolitically, and historically disruptive events

coming to nexus in Hamburg Germany, in 1985. The convergence of disruptive events created the environment necessary to make Operation EQUALIZER a reality, but it did not create the Cuckoo's Egg events in isolation. The Cuckoo's Egg investigation is a lens on cold-war realist grand strategy where the impact of information dominance, and the loss of it, comes into sharp focus as a result of amplified vulnerability resulting from the abstraction of physical security barriers and rapid development of interconnected network-computing systems. BND Project RAHAB and the CUCKOO'S EGG investigation existed in context with other major foreign intelligence service computer mediated espionage penetrations. The CUCKOO'S EGG investigation holds prominence in western media and literature, but other noteworthy computer virus attacks, and other technology development during the time period remain of equal importance. According to the National Counter Intelligence Center (NACIC) 1995 annual report to Congress on Foreign Economic Collection and Industrial Espionage, RAHAB-period techniques such as computer intrusion, telecommunications targeting and interception, and exploitation of weak private sector encryption and computing systems remains commonplace. According to the 1995 NACIC report, computer-mediated activities account for the largest part of economic and industrial information lost by U.S. corporations (18). Porteous (1993) argues that economic espionage is inexpensive to conduct and potentially cost-effective; and the resulting play-by-play account in Cliff Stoll's *The Cuckoo's Egg* lays that out in great detail. The potential benefits can be large and lasting. Although not calculated, the acquisition of the IBM 370 source code, cut the development time of the Soviet RYAD missile control operating system into a fraction of time it took IBM to build the IBM 370 from ideas and plans. Negative cash flow nations can use economic espionage to

achieve parity with an equivalent cash subsidy. The risk-benefit analysis favors the sponsoring government (8). BND Project RAHAB did exist, but it was not the hallmark computer-mediated espionage program of the time period, nor was it the first program to embrace computer-mediated espionage and hacking. The BND RAHAB program did not serve as the incubator cell for West German UNIX and VMS hacking activity in 1985-1986 – the CCC served that purpose. Project RAHAB was not related in any way to the CUCKOO'S EGG penetrations despite the perpetrators literally being "down the street" in a figurative sense. Last, incomplete facts exist over the BND's prowess in the field of computer-mediated espionage during 1981-1989. Additional research is in need.

## WORKS CITED


1. Adkins, B.N., Maj., USAF (2001) *The Spectrum of Cyber-Conflict from Hacking to Information Warfare: What is Law Enforcement's Role?* Document AU/ACSC/003/2001-04. Air Command and Staff College. Air University.

2. Atlas of Cyber Space (2004). *Historical maps of Computer Networks*. Internet. Found at http://www.cybergeography.org/atlas/historical.html. Accessed on 18 January 2007.

3. Brenner, S. and Crescenzi, A. (2006) *State Sponsored Crime: The Futility of the Economic Espionage Act (EEA).* Houston International Journal of Law. pp. 390-464. Spring. Westlaw. Citation 28 HOUJIL 389. Access on 22 September, 2006.

4. Defense Science Board (1996) *Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D).* November 1996. Office of the Under Secretary of Defense for Acquisition and Technology. Department of Defense. Washington D.C.

5. Fix, B. (1987) *Virus Auf Eiem Rechner IBM 3090 Unter Dem Betr.system MVS/370 Version 1*. [text output of assembler source code]. Internet. Found at http://www.aspector.com/~brf/devstuff/rahab/vp370.asm.html. Accessed on 10 April 2007.

6. Fix B. (2004) A Strange Story. Author's Internet Website 9 June 2004. . Internet. found at http://www.aspector.com/~brf/devstuff/rahab/rahab.html Access on 5 March 2007.

7. Fraumann, E. (1997) *Economic Espionage: Security Mission Redefined.* Public Administration Review. July-August 57(4) 303-308.

8. Madsen, W. (1993) *Intelligence Agency Threats to Computer Security*. International Journal of Intelligence and Counter-Intelligence. 6(winter). 413-445.

9. National Counter Intelligence Center (1995) *Annual Report to Congress: on Foreign Economic Collection and Industrial Espionage*. National Counter Intelligence Center. Washington D.C.

10. Office of the National Communications System (2000). *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP Internet Communications.* 1 December. Internet. Found at http://www.ncs.gov/library/reports/electronic_intrusion_threat2000_final2.pdf. Accessed on 14 February 2007

11. Porteous, S. (1993) *Commentary Number 32: Economic Espionage.* Canadian Security Intelligence Service [Service Candadien du Renseignment Desecurite]. Internet. Found at http://www.csis-scrs.gc.ca/en/publications/commentary/com32.asp. Access on 15 February 2007.

## BIBLIOGRAPHY

1. Mungo, P. and Clough, B. (1992). *Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals*. Faber and Faber, London.

2. Salus, Peter (1995). *Casting the Net: From ARPANET to INTERNET and Beyond*. First Edition. Addison-Wesley Publishing.

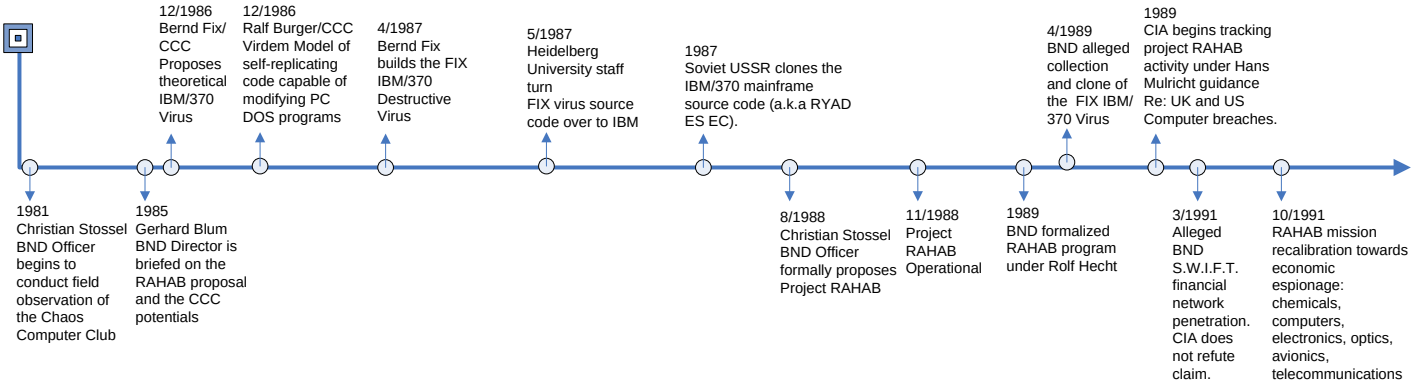
3. Schwiezer, Peter (1993). *Friendly Spies: How America's Allies are Using Economic Espionage to Steal Our Secrets.* . NY: Atlantic Monthly Press.

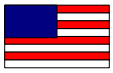
4. Stoll, Cliff (2000). *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage*. NY: Pocket Books.

# APPENDIX A: TIMELINE OF PROJECT RAHAB

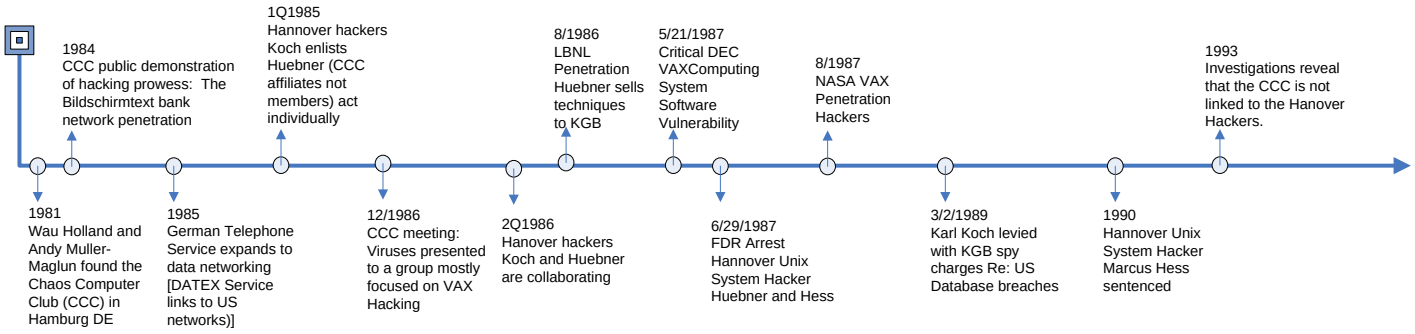
Appendix: Chronological Time Line Comparison: German BND Project RAHAB Development versus the Cuckoo's Egg Investigation

The chronological timeline leading to
German BND Project RAHAB computer mediated espionage developments



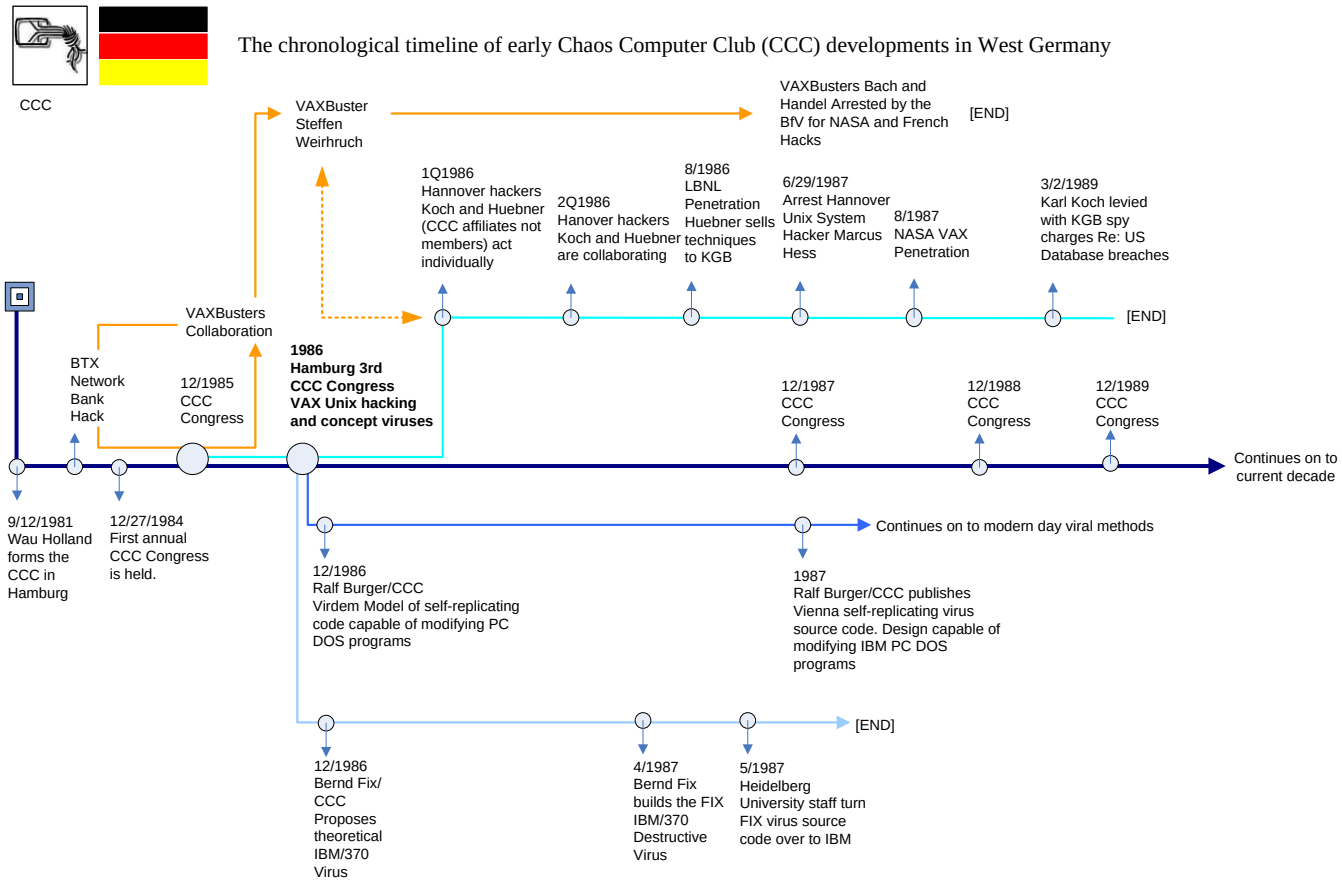
The chronological timeline leading to the
Cuckoo's Egg Lawrence Berkley National Laboratory computer penetration investigation




The diagram represents the Author's original analysis work. Unpublished

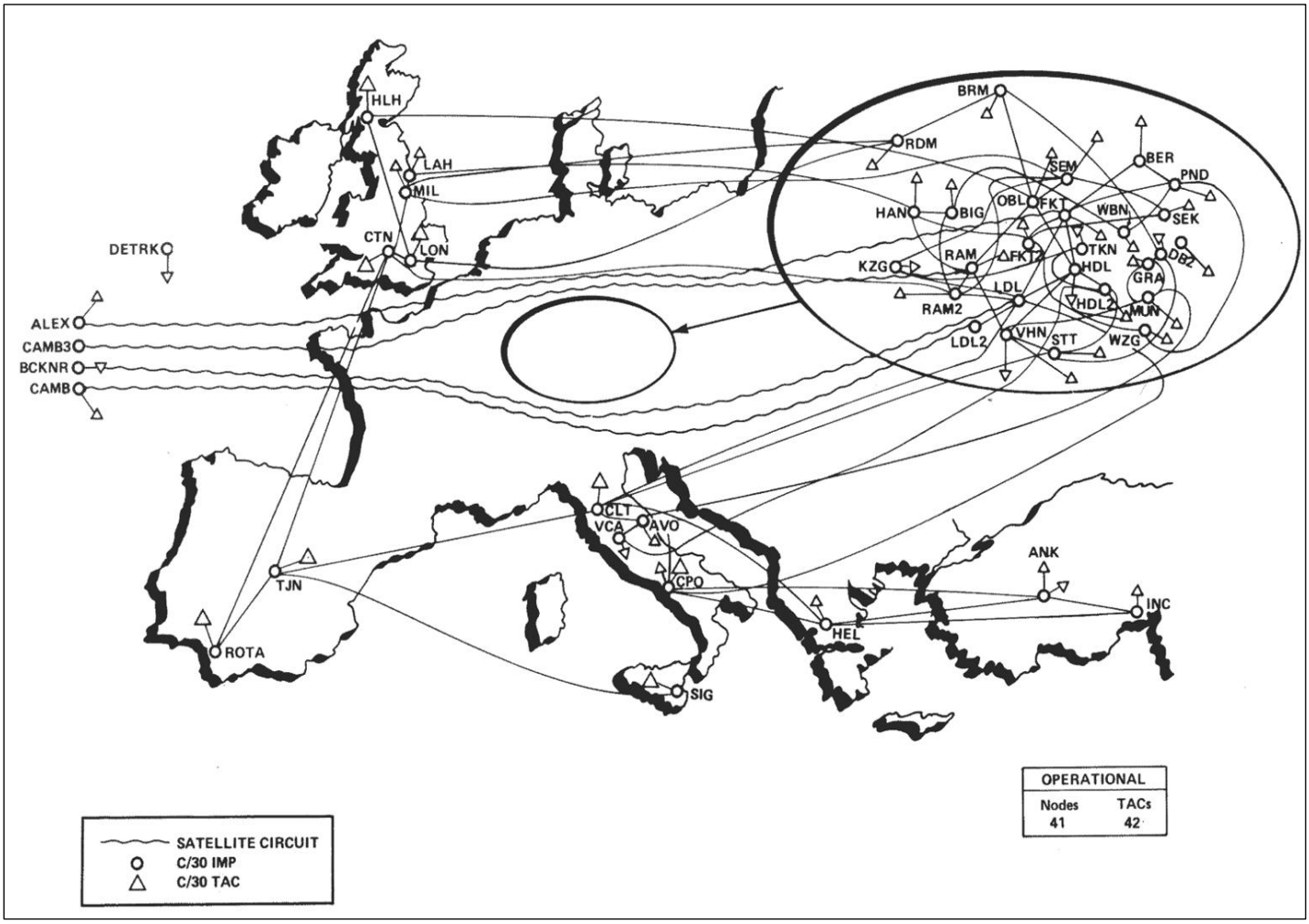
# APPENDIX B: TIMELINE OF THE CCC

Appendix: The chronological timeline of Chaos Computer Club (CCC) early developments in West Germany




The diagram represents the Author's original analysis work. Unpublished

## APPENDIX C: MILNET (Defense Data Network) as of 1989




Maps of MILNET (Defense Data Network) in the US and Europe, from 1989. MILNET split from ARPANET in 1984. (Source: Directory of Computer Networks, edited by Tracey L. Laquey, Digital Press, 1990). Reproduced at http://www.cybergeography.org/atlas/historical.html.