Intruder Investigation

PHASE 1

August - September, 1995

Multiple intrusions into military computer systems are noted by the Naval Criminal Investigative Service.

These are analyzed and linked to an unknown intruder using accounts on the Internet computer serving the Faculty of Arts and Sciences at Harvard University.

A profile is developed of the intruder, including the sites he has attacked, the accounts he has compromised, and the signature-like tools he has used to compromise the computer systems.

PHASE 2

October - December, 1995

The U.S. Attorney in Boston obtains authorization for the country's first court-authorized wiretap in the middle of a computer network.

To isolate the intruder's communications from those of the legitimate users of the Internet, a high speed computer is used to identify and record only those computer sessions which fit the intruder's profile.

After attacking a site in Taiwan through the Harvard computer network, the intruder is monitored while "chatting" on the Internet using the handle "griton." This and other attacks are traced back to a computer system in Buenos Aires, Argentina.

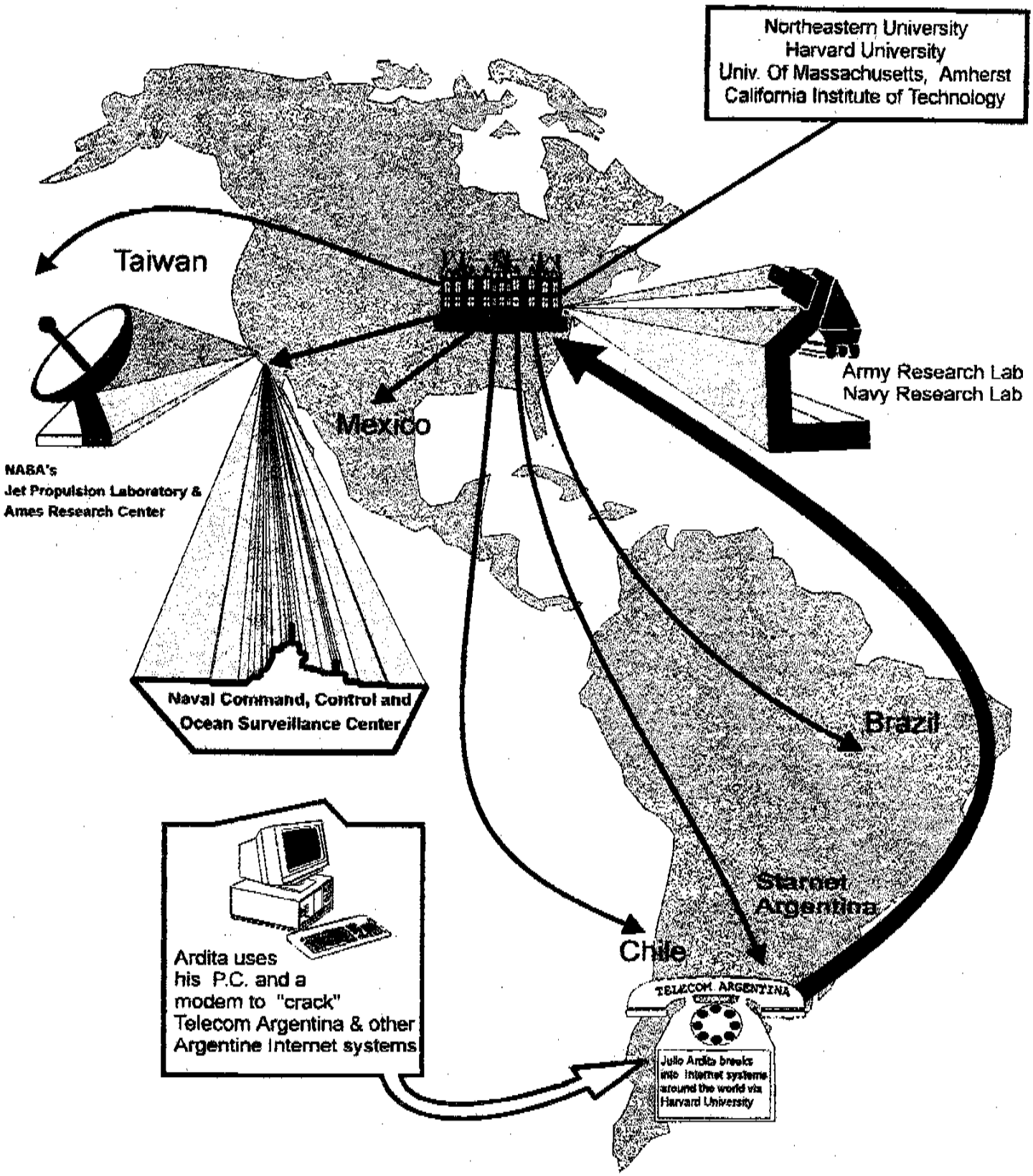
PHASE 3

January - February, 1996

Multiple Internet archives are searched for other appearances of "griton." "Griton" is found to have made a number of descriptive postings on a computer bulletin board frequented by hackers.

This information is correlated with information developed by the Argentine Federal Police and the Federal Bureau of Investigation.

"Griton" is identified as Julio Cesar Ardita, a system operator of a "pirate" computer bulletin board system which specialized in "hacking," "cracking" and "phone phreaking."


Northeastern University
Harvard University
Univ. Of Massachusetts, Amherst
California Institute of Technology
Taiwan
Army Research Lab
Navy Research Lab
Mexico
NASA's
Jet Propulsion Laboratory &
Ames Research Center
Naval Command, Control and
Ocean Surveillance Center
Brazil
Ardita uses
his P.C. and a
modem to "crack"
Telecom Argentina & other
Argentine Internet systems
Starnet
Argentina
Chile
TELECOM ARGENTINA
Julio Ardita breaks
into Internet systems
around the world via
Harvard University