Extent

3 folders, approximately 25 pages

Summary

This collection consists of records related to cyber warfare operations in conjunction with Operation Desert Fox in Iraq between December 16 and December 23, 1998. Cyber warfare is something quite new in the history of international conflict. In 1998, the administration released Presidential Decision Directive 63 (PDD/NSC-63) which addressed the increasing vulnerablity of computer networks and called for public and private partnerships to protect these systems. Following the release of PDD-63 and a number of successful attacks against American computer systems the administration was much more aware of the growing use of computers as a tool for terrorism or warfare. The collection contains open press articles on cyber warfare as well as FBI National Infrastructure Protection Center (NIPC) warning notices.

Scope and Content Note

The materials in FOIA 2014-1058-F are a selective body of documents responsive to the topic of the FOIA. Researchers should consult the archivist about related material. Freedom of Information Act (FOIA) request 2014-1058-F was for records related to cyber warfare operations in conjunction with Operation Desert Fox in Iraq between December 16 and December 23, 1998. The records to be opened include open press articles on cyber warfare as well as FBI National Infrastructure Protection Center (NIPC) warning notices. Cyber warfare is something quite new in the history of international conflict. NATO noted on its website, “Cyber-The Good, The Bad and the Bug Free: The History of Cyber Attacks—A timeline,” that it was not until the Morris virus in 1988 that there was a large scale attack on the world’s computer systems. Many journalists, historians, and academics note though that work toward exploitation of computer systems began as early as the 1970s. The focus remained, even into the 1990s, on intelligence gathering or protection of computer networks

not on attacking and disabling systems. This can be seen in the National Security Agency's Cray Supercomputers, the National Bureau of Standards, data encryption standards; or in the development of the Cryptographic Keying Device (KOK-1). Some who have studied cyber warfare note that it was not until the discovery of the Stuxnet virus in 2010 that anyone knew of a malware virus that could subvert infected systems. Time magazine ran an article, "Onward Cyber Soldiers" (August 21, 1995), in which they introduced the United States Army's Intelligence and Security Command (INSCOM). The article describes the efforts of the Army to deal with the "what ifs" of early cyber conflict. During the Clinton administration cyber activities and cyber warfare was all very new. This was, after all, the first administration to have widespread access by staff to e-mail and computers. The administration didn't even have a common language, referring to cyber warfare as information warfare, critical infrastructure, or variations on cyber. In 1997, the U.S. held a military exercise, Operation Eligible Receiver, which was focused primarily on computer warfare. The National Security Agency, acting as the hostile team, was able to compromise a number of government computer networks. By 1998, the administration released Presidential Decision Directive 63 (PDD/NSC-63) which addressed the increasing vulnerability of computer networks and called for public and private partnerships to protect these systems. Following Eligible Receiver, the release of PDD-63, and a number of successful attacks against American computer systems the administration was much more aware of the growing use of computers as a tool for terrorism or warfare. Richard Clarke and George Tenet both spoke, in 1998, about information warfare or cyber warfare as a tool of both the United States and those who would act against the United States. During Kosovo, the NATO peacekeeping effort and the United States faced a number of attacks on computer networks from hacker groups who supported the Serbians. It was not until the final years of the administration that the White House began to think in earnest of the threat and possibility of cyber warfare.

Record Type

Textual

System of Arrangement

Records that are responsive to this FOIA request were found in these collection areas—Clinton Presidential Records: NSC Cable, Email, and Records Management Systems.

Access

Collection is open to all researchers. Access to Clinton Presidential Records is governed by the Presidential Records Act (PRA) (44 U.S.C. Chapter 22, as amended) and the Freedom of Information Act (FOIA) (5 U.S.C. 552, as amended) and therefore records may be restricted in whole or in part in accordance with legal exemptions.

Copyright

Documents in this collection that were prepared by officials of the United States government as part of their official duties are in the public domain. Researchers are advised to consult the copyright law of the United States (17 U.S.C. Chapter 1) which governs the making of photocopies or other reproductions of copyrighted material.

Provenance

Official records of William Jefferson Clinton’s presidency are housed at the Clinton Presidential Library and administered by the National Archives and Records Administration (NARA) under the provisions of the Presidential Records Act (PRA).

Processed by

Staff Archivist, 2016. Previously restricted materials are added as they are released.

Last Modified Date

2016-06-15

Container List

The following is a list of documents and folders processed in response to FOIA 2014-1058-F.
Box 1
Clinton Presidential Records: NSC Cable, Email, and Records Management System
NSC Cables
Jan 1997-Dec 1998 [OA/ID 520000]
[Cyber, Iraq]
[12/18/1998-12/22/1998]
NSC Email
Exchange-Record (Sept 97-Jan 01) [OA/ID 620000]
[Cyber, Iraq]
[12/18/1998-12/21/1998]
Exchange-Non-Record (Mar 97-Jan 01) [OA/ID 630000]
[Cyber, Iraq]
[12/18/1998]