NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

A HONEYPOT FOR SPIES: UNDERSTANDING INTERNET-BASED DATA THEFT

by

Blake T. Henderson

December 2018

Thesis Advisor:	Neil C. Rowe
Second Reader:	Victor R. Garza

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
A HONEYPOT FOR SPIES: UNDERSTANDING INTERNET-BASED DATA THEFT

5. FUNDING NUMBERS

6. AUTHOR(S) Blake T. Henderson

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Creating ruses and planting false documents to deceive our adversaries is a tactic that has been used for a long time. Honeypots allow us to easily plant false data on information systems while we monitor what attackers access and download. This enables us to learn of a potential spy's interests and intents, helping defenders decide how to concentrate their resources when protecting critical information networks. In this thesis, we used a content-based Web honeypot to monitor access to military-related documents to see what type of information Internet users were most interested in obtaining. We created a webserver within the Naval Postgraduate School address range, mimicked the Naval Postgraduate School library's website layout, and used webpage and webserver log monitoring software to analyze activity. We characterized both human and automated (bot) activity and found that the cyber subpage was the most popular among both types of users. Additionally, human-user document downloads tended to be in order of appearance on the webpage (alphabetically), but bot-user downloads appeared to be more random.

14. SUBJECT TERMS
honeypot, electronic counterintelligence, deception, data theft

15. NUMBER OF PAGES
103

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

A HONEYPOT FOR SPIES: UNDERSTANDING INTERNET-BASED DATA THEFT

Blake T. Henderson
Lieutenant, United States Navy
BS, Brigham Young University, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
December 2018

Approved by: Neil C. Rowe
Advisor

Victor R. Garza
Second Reader

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Creating ruses and planting false documents to deceive our adversaries is a tactic that has been used for a long time. Honeypots allow us to easily plant false data on information systems while we monitor what attackers access and download. This enables us to learn of a potential spy's interests and intents, helping defenders decide how to concentrate their resources when protecting critical information networks. In this thesis, we used a content-based Web honeypot to monitor access to military-related documents to see what type of information Internet users were most interested in obtaining. We created a webserver within the Naval Postgraduate School address range, mimicked the Naval Postgraduate School library's website layout, and used webpage and webserver log monitoring software to analyze activity. We characterized both human and automated (bot) activity and found that the cyber subpage was the most popular among both types of users. Additionally, human-user document downloads tended to be in order of appearance on the webpage (alphabetically), but bot-user downloads appeared to be more random.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ASP	application service provider
CIA	Central Intelligence Agency
DNS	domain name system
GB	gigabyte
HTML	hypertext markup language
HTTP	hypertext transfer protocol
IP	Internet protocol
ISP	Internet service provider
KGB	Komitet Gosudarstvennoy Bezopasnosti (Committee for State Security)
NATO	North Atlantic Treaty Organization
NPS	Naval Postgraduate School
PDF	portable document format
PHP	hypertext preprocessor
RAM	random access memory
RFC	request for comments
SSH	secure shell
URI	uniform resource identifier
URL	uniform resource locator

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Karen Kerno for her help in designing and creating our webpage and our honeypot’s external links. She was instrumental in our experiment’s success and her assistance was far beyond our expectations.

I am grateful for Dr. Neil Rowe and his steady guidance. He allowed me to lead the way during our research and experimentation and pointed me in the right direction when I needed it.

I am so thankful for my wife, Sara, and her unwavering patience through many late nights during this process. She took care of everything so that I could take care of this. And I can’t forget Olivia and Brock…the perfect distraction from schoolwork.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Countless foreign actors are working to exploit Department of Defense unclassified and classified networks, and some already have the capacity to disrupt the critical communication infrastructure (Department of Defense, 2011). When a close-knit community of researchers first developed the forerunner to the Internet roughly fifty years ago, they did not anticipate how much it would become an integral part of the world, and that it would even become a primary warfare domain. Additionally, they had no reason to mistrust each other and therefore did not bother complicating their system with security protocols (Gartzke & Lindsay, 2015). Information systems have become the backbone of institutions worldwide, promoting rapid growth and prosperity by providing unprecedented information resource availability.

Consequently, this reliance on the Internet and information systems leaves individuals, businesses, militaries, schools, and governments vulnerable to dangerous cyber threats (Department of Defense, 2015). Potential U.S. adversaries have taken advantage of these vulnerabilities to undercut U.S. operations, capabilities, and competitiveness while posing hostile threats to national interests (Department of Defense, 2015). Subsequently, the Department of Defense Cyber Strategy of 2015 says its primary cyber mission is to defend its own networks, systems, and information.

A. MOTIVATION

Network security is limited by monetary and time costs as well as convenience. Aside from unplugging essential hardware, no network will be completely secure (Singer & Friedman, 2014). Therefore, cost-based and usability decisions drive the level of network protection for information. In 2010 the U.S. government had more than 15,000 networks and over seven million connected devices dispersed over hundreds of installations all over the world (Lynn, 2010). Because the number of networks and connected devices are likely significantly higher today, securing U.S. government information is an ambitious task.

Attackers use the anonymity of Internet personas to steal data without attribution. However, honeypots allow us to set up test environments in which we can monitor the activity of network intruders and control the content they access. A honeypot is a controlled computing resource that is designed to be probed, attacked, or compromised (Provos, 2004). A honeypot's value is in its vulnerability to being probed and attacked, and any interaction with the honeypot can be characterized as malicious (Spitzner, 2002). Normal users would have no reason to interact with a honeypot and would likely be unaware of its existence. A Web-based honeypot can provide a platform for counterintelligence against adversary spies collecting information.

Deception strategies for information systems are beneficial today just as they have been in warfare throughout history. The Chinese strategist Sun Tzu famously stated that all war is based on deception (Sun Tzu, 1971), and in the information age, the United States is facing a form of silent and sometimes non-attributable warfare through cyber-attacks and cyber espionage. Historically, military deception campaigns have been very effective at adding to the overall friendly security posture and understanding of adversary intents. Counterintelligence and deception efforts do not replace security but enhance an overall security posture in the long run.

B. OBJECTIVES

The intent of this thesis is to more specifically develop methods to identify the most enticing types of military-related documents sought after by adversaries. This will help defenders decide how to concentrate their resources when protecting critical information networks. The focus is to determine the categories and content of documents that adversaries are most actively pursuing to collect. This thesis used a honeypot resembling webpages associated with the Naval Postgraduate School's Dudley Knox Library, but it was not readily accessible to the average Dudley Knox Library user. Only those digging for information to scrape from the Naval Postgraduate School could encounter the honeypot, where their activities were monitored and logged for post analysis.

The logs of the users' interaction with the honeypot, paired with the source Internet Protocol address geographic information, gave insights into which countries tend to hunt for each category of information. To build the honeypot, we categorized unclassified open-source documents and aggregated them by type, and posted the documents into clickable subdomains. Each subdomain contained technical and policy-related documents organized by the nature of their subject.

Discerning what information adversaries most desire is important for network security. System administrators are constantly challenged by the persistent threat of data theft from the networks they are charged with protecting. Internet-based data theft affects private and public organizations alike, but the United States government is a particularly lucrative target. By combining deception with data, we may potentially conduct counterintelligence on adversaries trying to compromise Department of Defense networks.

C. THESIS STRUCTURE

This thesis will examine Internet-based document collection to help focus U.S. government cyber security efforts. Chapter II covers background, honeypots, the legality of honeypots, previous work detecting Internet-based data theft, and previous work using honeypots. Chapter III covers the problem being solved, the modeled environment and assumptions, and similar work. Chapter IV presents our methodology, content selection and criteria, honeypot setup and activation, and data collection. Chapter V presents our summary and interpretation of results and the performance of our chosen methodology. Chapter VI discusses our conclusions and proposes future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND AND PREVIOUS WORK

A. INTELLIGENCE AND COUNTERINTELLIGENCE

The Office of the Director of National Intelligence defines intelligence as information "gathered within or outside the United States" that involves "threats to the U.S., its people, property, or interests" (Office of the Director of National Intelligence, 2011). The United States government uses intelligence to determine the consequences of security and policy decisions that could have long-term effects. Likewise, adversaries collect intelligence on the United States for their own purpose of furthering their interests. The United States also conducts counterintelligence to protect U.S. activities and institutions from infiltration by hostile foreign organizations and individuals. Counterintelligence is any activity associated with collecting, organizing, understanding, or responding to intelligence threats from an adversary to avoid sensitive or classified information from being compromised (Rodriguez-Hernandez, 2013). The main goal of counterintelligence is to neutralize enemy intelligence collection and protect national information. Intelligence and counterintelligence efforts use human and technological methods to form the first line of defense for military and national institutions.

While counterintelligence has been practiced for centuries, its use in information systems is relatively new. The basic principles of digital deception and digital counterintelligence evolved from techniques practiced in traditional warfare. During the American Revolutionary War, Captain David Gray of Massachusetts posed as a deserter and entered the service of a Tory intelligence officer named Colonel Beverly Robinson (Rafalko, 2004). Gray became Robinson's courier, which enabled the Americans to read each of Robinson's dispatches before their delivery to the intended recipient. During the same war, Paul Revere and the Sons of Liberty discovered that the British planned to march on Lexington and Concord by observing the British soldiers' movements.

Counterintelligence also includes planting false documents to mislead the adversary about our own intentions. Planting fake documents to mislead an enemy has become commonly referred to as a "haversack ruse." This term came about following the

1917 British deception operation against the Turks during World War I (Coyle & Wilson, 2014). A British officer feigned an injury and dropped his bloody haversack along with his rifle and water supply. His haversack contained false classified documents regarding an upcoming attack on Gaza. Among the British officer's "lost" documents were money, a letter from his wife, and a photograph of his recently born child. The personal documents and artifacts successfully supported the believability of the classified documents. The Turkish and German militaries prepared for an upcoming attack against Gaza while the British went on to victory in Beersheba, ending a longstanding stalemate.

Such ruses using fake documents continued throughout World War II. Famously, the Allies planted a dead body off the coast of Spain as part of Operation Mincemeat (Bacon, 1998). The body was dressed so that he appeared to be a courier that had drowned after falling from an Allied ship. The body had a briefcase attached that contained documents specifying Allied plans to invade Europe through Greece. The Spanish sent this intelligence to the Germans who then misallocated their defenses in the Mediterranean.

The Allies attempted another deception operation during Operation ERROR in Burma in April 1942 (Coyle & Wilson, 1942). General Archibald Wavell, Commander-in-Chief, Allied Forces in the Southwest Pacific, purportedly left his briefcase in his Ford Mercury staff car after a crash while fleeing the Japanese. In his haste, General Wavell left his briefcase and personal items, including family photographs, with the intent to deceive the Japanese into believing that Allies had many more troops in India than they actually did. The Allies' intent was to discourage the Japanese from invading India.

The cyber realm makes deception cheaper and easier than it was in previous eras. Furnishing falsified documents for adversaries to find can be accomplished easily within minutes. Deception is "essential for intelligence gathering about an adversary" and cyber deception "should tell the adversary what they want to know" (Rowe & Rrushi, 2016). Planting false documents can hamper an adversary's productivity by wasting intelligence collection resources. As a complement to defense, deception is often inexpensive to deploy but costly for adversaries to overcome. Hackers regularly steal valuable information from institutions, so it is feasible to run a deception operation allowing attackers to exfiltrate misleading information (Bodmer, Kilger, Carpenter, Jones, & Jones, 2012). Additionally, digital deception operations are more practical nowadays, as navigating a proposal such as Operation Mincemeat through modern military channels would be near impossible.

In the 1980s the Central Intelligence Agency (CIA) was aware that the Soviets were stealing important technology documents (Weiss, 2007). Because the CIA was unable to stop the exfiltration of data, modified versions of the technology were "made available" to sabotage Soviet technology production. Even if the Soviets discovered the intent of the modifications, it would be good because they would have reason to doubt every document and source of technology that they had received. By providing false or misleading documents through our information systems, we can dissuade enemies from trusting even the valid documents they obtain.

Counterintelligence allows us to learn about our enemies and their intentions. Counterintelligence is not the same as security, but they are related (Johnson, 2009). By studying a spy's interests, tactics, techniques, and procedures, network managers may be able to bolster the security of their networks. Honeypots are counterintelligence tools deployed on information systems and are designed to lure intruders, collect intelligence about them, and deceive them about the true nature of the environment (Schmitt, 2013).

B. HONEYPOTS

A honeypot is a "security resource whose value lies in being probed, attacked, or compromised" (Spitzner, 2002). Furthermore, honeypots are resources that have no production value, so therefore no person or resource should be communicating with them. Honeypots are flexible tools that can be adapted and applied to different situations. Spitzner distinguishes two categories of honeypots: production and research.

- Production honeypots are designed to help secure an environment, for example, by detecting attacks. They add value to network security and support risk mitigation but provide less detail than research honeypots about the attackers and their attacks.
- Research honeypots collect data about attackers. Their purpose is to help an organization understand threats and how they operate. Research honeypots help secure an organization's resources indirectly.

1. Honeypot Interaction Levels

Honeypots can be low-interaction, medium-interaction, or high-interaction (Joshi & Sardana, 2011) (Figure 1). Low-interaction honeypots typically emulate services like FTP or HTTP, but do not provide real operating systems or services. They are simple to deploy and maintain but provide limited information about the attacker. Medium-interaction honeypots do not have real operating systems but a layer of virtualization providing hackers with expected responses to lure them to attack; defenders can then record and study attack payloads. High-interaction honeypots provide access to real operating systems and provide the ability to collect the highest amount of information about an attack. They are the highest risk because they expose an entire system to an attacker. A limited form of a high-interaction honeypot is used in this thesis.

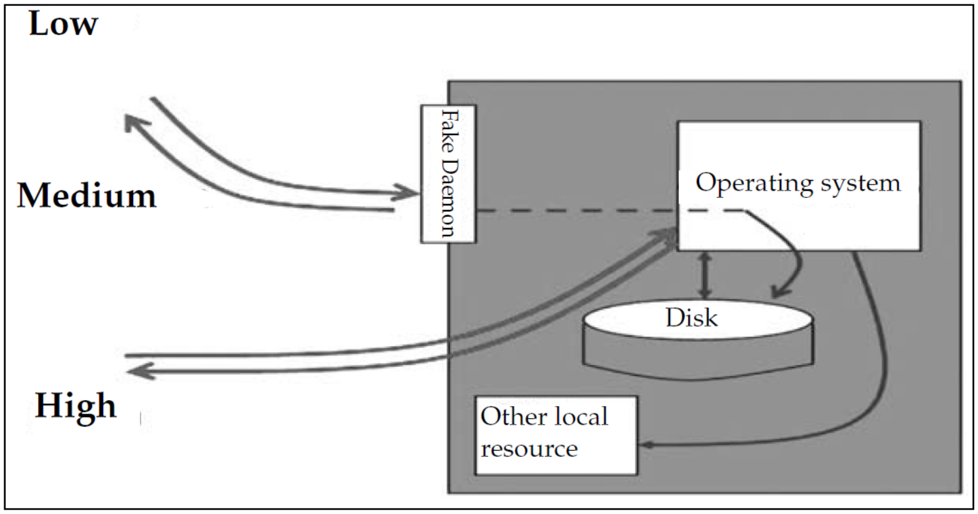


Figure 1. Honeypot classification by level of interaction. Source: Joshi and Sardana (2011).

2. Legality of Honeypots

Honeypots are permitted under Rule 61 of the Tallinn Manual on the International Law Applicable to Cyber Warfare (Schmitt, 2013). The Tallinn Manual is a document sponsored by the NATO Cooperative Cyber Defense Centre of Excellence and written by an independent international group of cyber experts. It is the most widely accepted manual on law governing cyber warfare. Rule 61 states that operations that qualify as ruses are permitted, including false computer and device identifiers, honeypot computer networks, and false digital transmissions. This rule asserts that transmitting false intelligence information intended for enemy interception is permitted. Additionally, the Tallinn Manual describes the purpose of honeypots as enticing intruders to waste resources on the decoy environment. It states that honeypots enable gathering counterintelligence about the intruders' intent, identity, and methods of cyber operations.

C. DETECTING INTERNET-BASED DATA THEFT

Before honeypots were common, a manager at the Lawrence Berkeley Lab was one of the first to track and record the activities of a hacker (Stoll, 1990). Stoll's supervisor tasked him to track down a 75-cent shortfall from the previous month's $2,387 Unix computing system bill. This turned out to be caused by a hacker's unauthorized use of the system. Over several months, Stoll used dozens of computers, monitors, and printers to track and log the hacker's activity. Stoll created files that seemed interesting and put them in a directory that only the attacker would be able to access. The result was that the hacker stayed on the system for more than two hours downloading the bogus documents, which was long enough for the authorities to trace the call. Stoll's efforts eventually led to the arrest of a German hacker who had been stealing information from the U.S. government and selling it to the KGB.

Another early honeypot was created at AT&T Bell Laboratories (Cheswick, 1992). Cheswick observed a hacker attempt to email himself a copy of the password file from an Internet-gateway computer using a well-known vulnerability. The hacker's attempt failed, but Cheswick emailed the hacker a false password file anyway. Cheswick then created a simulated system (what is now called a "sandbox") so that he could observe and learn more about the attacker. When the attacker attempted to erase all the files on the simulated system, Cheswick built what he called a jail for the attacker. Cheswick loaded the file system with tempting files that were not very convincing but observed that this did not deter the attacker. After months of toying with the hacker, Cheswick concluded that monitoring a sandbox with real security vulnerabilities was a viable method to deter a hacker from attacking the real system.

D. PREVIOUS WORK USING HONEYPOTS

Honeypots have evolved over the last twenty-five years and are common tools in research and network defense. Typically, honeypots do not address a particular problem but are instruments in the overall security architecture (Anuar, Zakaria, & Chong, 2006). Anuar et al. suggest the following:

1. Honeypots can be generic but should mimic the information system environment. When networks change, honeypots should reflect the changes.

2. Honeypots should entice attackers with seemingly genuine and stimulating information. This will encourage attackers to stay in the honeypot longer while network defenders monitor their actions. It can be particularly good to simulate an intranet server to further entice the attacker.

3. Everything collected through a honeypot is valuable, as it leads to a better cognizance and comprehension of network security. Recording an attacker's activity provides insight to potential system vulnerabilities and attacker techniques.

4. Honeypots should be designed so that attackers cannot use them as a launch pads for further attacks.

Honeypots should also respond so that the attacker believes that the exploit succeeded (Altwaijry & Shahbar 2013). They observed that most attacks that arrived at the honeypot could not be detected by an attack signature, so the honeypot data was valuable. Advantages of honeypots are (Spitzner, 2002):

1. Low false positives: Any activity on a honeypot is unauthorized and likely an attack.

2. Flexibility: Honeypots are easily customizable for different environments and threats.

3. Resources: Honeypots can be deployed with minimal resources even on large networks.

Disadvantages of honeypots are the risk that attackers can potentially use a honeypot to attack non-honeypot systems on the network, and their narrow field of view, i.e., that honeypots only collect data on what interacts with them (Spitzner, 2002). Another disadvantage is that attackers, even automated ones, will leave a computer system if they suspect a honeypot (Rowe, 2006). Automated attacks will often look for visualization technology and virtual-machine software signatures as signs of a honeypot. Honeypots are more effective the more ordinary they appear, and using deception and counterdeception are ways to maximize leverage in a situation limited by fixed resources.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PROBLEM DEFINITION AND ASSUMPTIONS

A. PROBLEM DEFINITION

It is important that network administrators and defenders know where and how to allocate their time and resources to protect critical information. In most cases, network defenders learn of a spy's origin and interests only after a successful compromise. Honeypots offer defenders clues that enable them to find out what the adversary is interested in (Rowe, 2018). Additionally, honeypots can distract intelligence collectors from legitimate resources at low cost. Defenders playing a multi-period game can attain cost-effective security through covertness and deception (Zhuang, Bier, & Alagoz, 2009). An attacker is less likely to attack if the information sources cannot be fully trusted. Honeypots also enable network defenders to cost-effectively collect information about attackers over extended time periods.

To test these principles on a Department of Defense network, we researched the efficacy of a content-based honeypot using a webserver with a Naval Postgraduate School IP address. This provided us with a unique opportunity to test cyber-deception tactics because honeypots are not regularly employed cybersecurity tools on Department of Defense networks. We monitored traffic of the webserver, which provided a variety of Department of Defense technical and policy related documents.

For this study, we were interested in finding out if foreign intelligence actors were collecting information from Naval Postgraduate School websites. We were unable to use an authentic Naval Postgraduate School domain name, so we tried to convince users of our website's authenticity by closely mimicking the format of the legitimate school library websites. We also ensured that our webserver was hosted within the Naval Postgraduate School Internet Protocol range.

B. RELATED WORK

Related research used an enhanced collection scheme on high-interaction Web honeypots in an effort to improve collection of attack information (Yagi, Tanimoto, Hariu, & Itoh, 2010). They found that 97 percent of attacks on their Web honeypot failed but that

50 percent of the attackers eventually succeeded. When a path defined in the attacker's destination URL did not exist, the researchers used an algorithm to convert the URL to a correct path. This improved the quantity of useable information collected with the Web honeypot.

An aggressive Web application honeypot can expose attackers' identities by giving them malicious JavaScript code that runs on the attacker's host when an attacker opens a honeypot website. Some work (Djanali et al., 2014) emulated an institutional news website containing software vulnerabilities and multiple pages with false information and fake articles. They also created a Facebook page that was unintentionally liked by the attacker if he or she was logged into his or her Facebook account when they visited the honeypot. They noted that users of the same spoken language as the fake website were easier to attract.

Other research performed graph-based analysis of a Web honeypot's log to help forensic investigators understand cyberattacks (Studiawan, Djanali, & Pratomo, 2016). They stored the attackers' attributes consisting of HTTP connection data including remote address, timestamp, request, referrer, user agent, and origin country and city along with the attack type. This helped investigators determine how many and what type of attacks were attempted from each area of the world.

Another project focused on the setup and deployment of a high-interaction honeypot to analyze the behavior of human attackers on the Internet. (Nicomette, Kaâniche, Alata, & Herrb, 2011). They ran an SSH server using a Gnu Linux operating system with a deliberate vulnerability of weak passwords. Their honeypot focused on observing and collecting information about non-automated attacks to gain more information on human behavior. They concluded that most attackers were trying to compromise systems for use in botnets. Because so many Internet-based attacks are conducted automatically by bots, capturing the activity of human attackers helped reveal plans and attack motivation.

Another project automated the creation of fake documents called Canary Files that are placed among real documents. Their purpose is to aid early detection of unauthorized data access, copying, or modification (Whitham, 2013). Canary files have no production value and network users should not need to access them. Whitham concluded that Canary Files generate less high-priority alerts than traditional data loss prevention systems and are most effective against advanced threat actors who try hard to avoid triggering alarms.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. METHODOLOGY

A. SETUP

We began building a honeypot for potential cyber spies by selecting fields of interest that are covered by the Department of Defense and the Naval Postgraduate School. We selected eleven document categories: air, space, cyber, military science & technology, surface warfare, subsurface warfare, special military operations, weapons systems, declassified projects, military budgets, and military policy. Next, we selected 132 documents (Appendix A) to host on our honeypot website. Each of the eleven categories contained ten to fourteen unclassified documents, most published within the last five to ten years. However, the declassified-projects documents were older because of United States government policies on document classification. Additionally, some of the declassified-projects documents were purged of sensitive information prior to public release. All documents used in our research were unclassified and publicly available.

We collected documents for our honeypot by conducting online queries through the Dudley Knox Library, Google Scholar, the CIA's online library, IEEE Xplore Digital Library, NASA HQ Library, and ScienceDirect. We used the honeypot category titles as keywords in our search for honeypot documents and reviewed each document to determine its suitability for inclusion.

Because the Naval Postgraduate School is a research institution, we selected technical and scientific documents within each category. Additionally, we selected budget documents that pertained to recent and future Department of Defense budget plans, and policy documents that highlighted foreign-policy challenges associated with China and Russia. By aggregating the documents on a web server associated with the Naval Postgraduate School, the intended inference we wanted would-be attackers to make was that there was Department of Defense interest in these subjects and that the documents were of value to potential intelligence collectors.

For the experiment, we installed a Linux 64-bit Ubuntu operating system and Apache 2.4.18 HTTP server software on a Dell Optiplex 960 desktop computer with 3 GB of RAM and a 312 GB hard disk. We opened port 80 for normal web traffic and port 22 to enable administrative SSH connections. We used a 19-character password, without dictionary words or repeating characters, to reduce the vulnerabilities of an SSH compromise, and made regular operating-system updates. Figure 2 shows our network connection to the Internet.

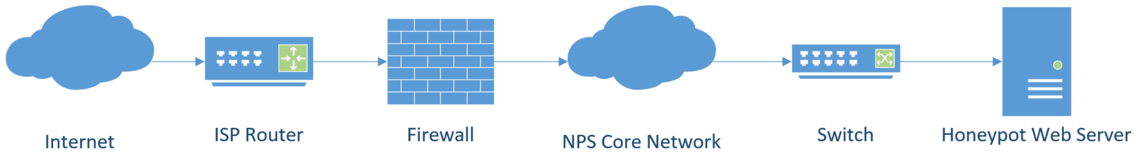
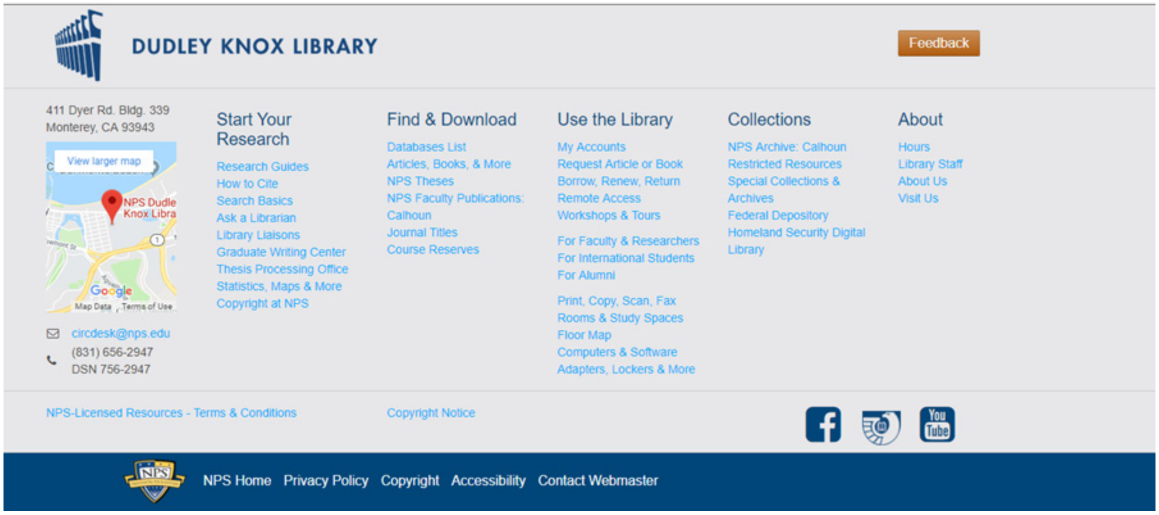


Figure 2. Honeypot network configuration.

We used 13 different HTML files to list our hosted content on the web server. The HTML files consisted of an index file, a site map, and one file for each of the 11 document categories. To suggest legitimacy, we used the same website header and footer as real websites at the Naval Postgraduate School and provided links to real Naval Postgraduate School webpages. The honeypot website footer is shown in Figure 3. We worked with a Naval Postgraduate School web-services librarian to ensure our honeypot website had a look and function similar to the real Naval Postgraduate School Library websites. The honeypot homepage is shown in Figure 4.



DUDLEY KNOX LIBRARY

Feedback

411 Dyer Rd. Bldg. 339
Monterey, CA 93943

circdesk@nps.edu
(831) 656-2947
DSN 756-2947

Start Your Research
- Research Guides
- How to Cite
- Search Basics
- Ask a Librarian
- Library Liaisons
- Graduate Writing Center
- Thesis Processing Office
- Statistics, Maps & More
- Copyright at NPS

Find & Download
- Databases List
- Articles, Books, & More
- NPS Theses
- NPS Faculty Publications: Calhoun
- Journal Titles
- Course Reserves

Use the Library
- My Accounts
- Request Article or Book
- Borrow, Renew, Return
- Remote Access
- Workshops & Tours
- For Faculty & Researchers
- For International Students
- For Alumni
- Print, Copy, Scan, Fax
- Rooms & Study Spaces
- Floor Map
- Computers & Software
- Adapters, Lockers & More

Collections
- NPS Archive: Calhoun
- Restricted Resources
- Special Collections & Archives
- Federal Depository
- Homeland Security Digital Library

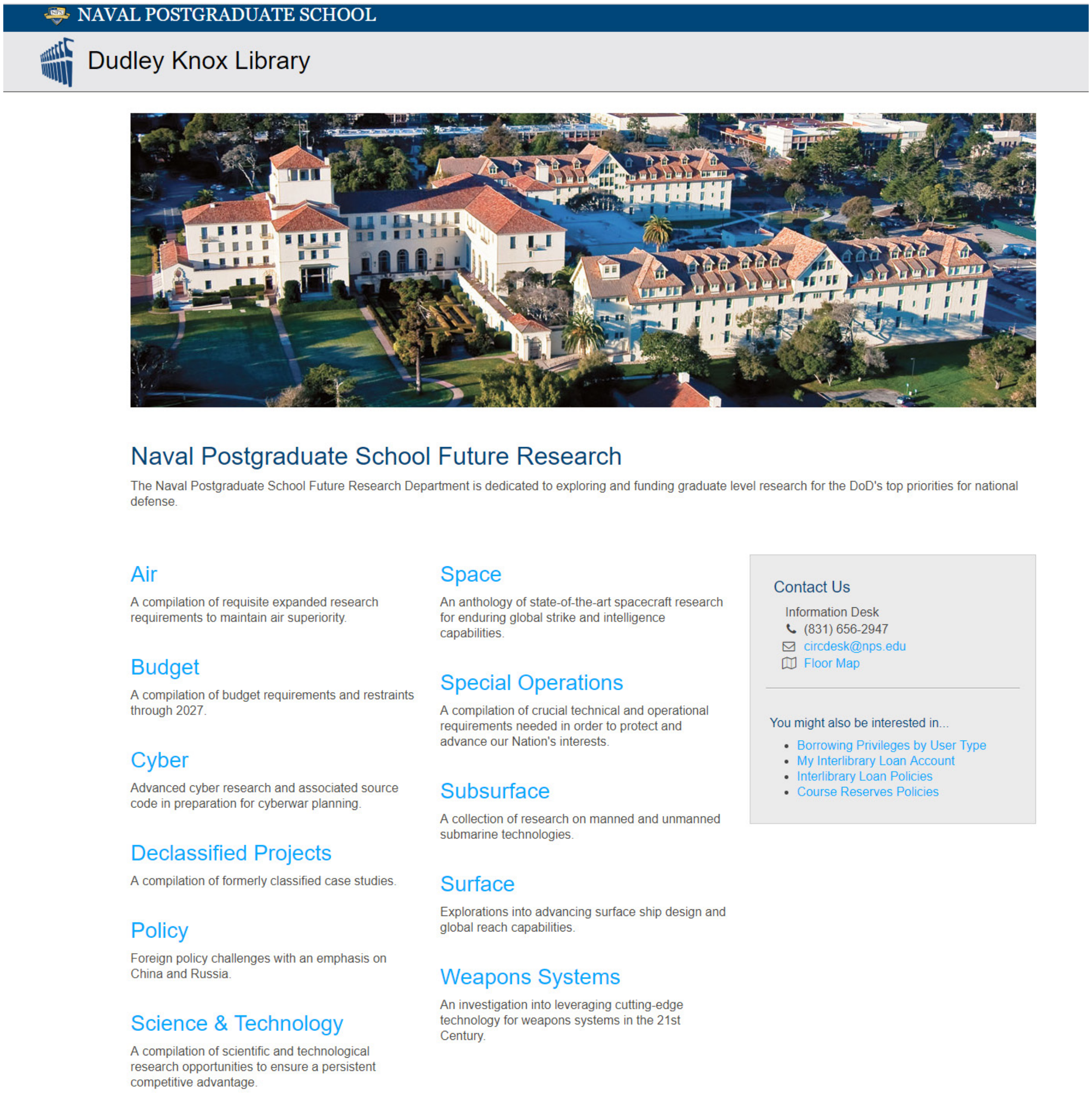
About
- Hours
- Library Staff
- About Us
- Visit Us

NPS-Licensed Resources - Terms & Conditions

Copyright Notice

NPS Home Privacy Policy Copyright Accessibility Contact Webmaster

Figure 3. Screenshot of honeypot website home page footer, with functioning links to NPS library websites.



NAVAL POSTGRADUATE SCHOOL

Dudley Knox Library

Naval Postgraduate School Future Research

The Naval Postgraduate School Future Research Department is dedicated to exploring and funding graduate level research for the DoD's top priorities for national defense.

Air

A compilation of requisite expanded research requirements to maintain air superiority.

Budget

A compilation of budget requirements and restraints through 2027.

Cyber

Advanced cyber research and associated source code in preparation for cyberwar planning.

Declassified Projects

A compilation of formerly classified case studies.

Policy

Foreign policy challenges with an emphasis on China and Russia.

Science & Technology

A compilation of scientific and technological research opportunities to ensure a persistent competitive advantage.

Space

An anthology of state-of-the-art spacecraft research for enduring global strike and intelligence capabilities.

Special Operations

A compilation of crucial technical and operational requirements needed in order to protect and advance our Nation's interests.

Subsurface

A collection of research on manned and unmanned submarine technologies.

Surface

Explorations into advancing surface ship design and global reach capabilities.

Weapons Systems

An investigation into leveraging cutting-edge technology for weapons systems in the 21st Century.

Contact Us

Information Desk
☎ (831) 656-2947
✉ circdesk@nps.edu
Floor Map

You might also be interested in...

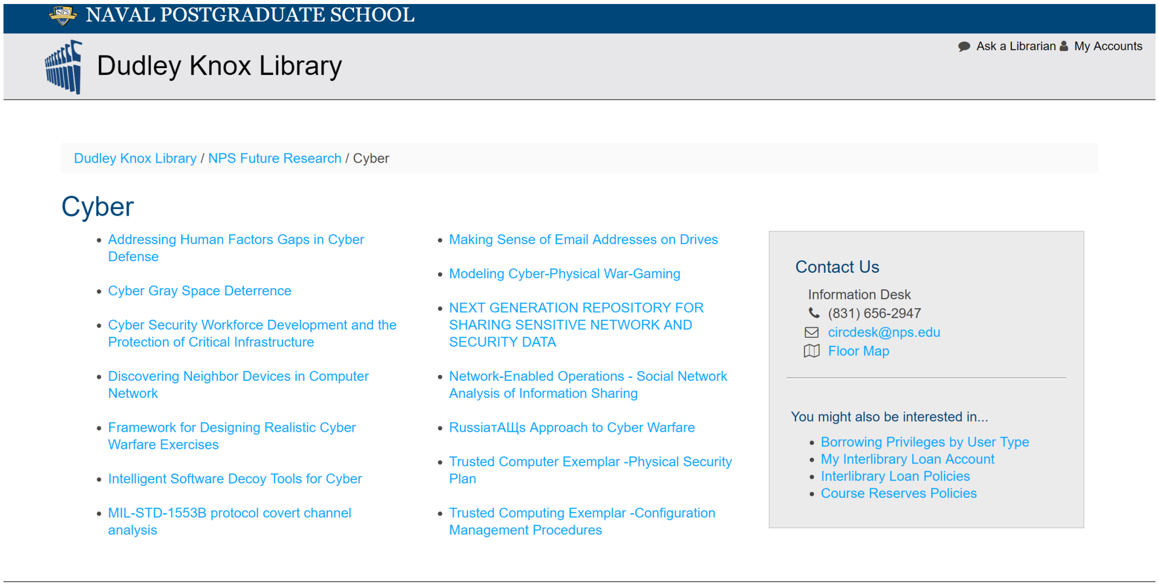
- Borrowing Privileges by User Type
- My Interlibrary Loan Account
- Interlibrary Loan Policies
- Course Reserves Policies

Figure 4. Screenshot of honeypot website home page.

We hosted the honeypot website on an IP address within the block of addresses owned by the Naval Postgraduate school so that a “whois” lookup confirmed our IP’s authenticity. However, we could not use an authentic Naval Postgraduate school URL ending in @nps.edu, so we chose the domain name www.nps-future-research.org. Using a different domain name extension than the actual library sites detracted from our honeypot’s authenticity, but we believe our IP address and website appearance helped compensate for this shortcoming.

Each category heading was a clickable link to subpages where we hosted the honeypot documents. We stored the documents as PDF files. To encourage further honeypot exploration into our subpages, we included a brief description of each category on the homepage. Each subpage had the same style as the honeypot homepage with functioning links to real Naval Postgraduate School library webpages. Figure 5 shows the Cyber subpage.

For potential spies to find our honeypot, we had to make our website visible on the Internet. We registered our domain name with Google so that Googlebot would index our honeypot website for the Google search engine. Then we created a structured sitemap (Appendix B) using xml-sitemaps.com, a sitemap creation tool, to enable search-engine crawlers to find and index our webpage content, subpages, and hosted documents. This allowed intelligence collectors to find our website through popular Internet search engines such as Google, Bing, Yahoo, and DuckDuckGo.



NAVAL POSTGRADUATE SCHOOL

Dudley Knox Library

Ask a Librarian My Accounts

Dudley Knox Library / NPS Future Research / Cyber

Cyber

- Addressing Human Factors Gaps in Cyber Defense
- Cyber Gray Space Deterrence
- Cyber Security Workforce Development and the Protection of Critical Infrastructure
- Discovering Neighbor Devices in Computer Network
- Framework for Designing Realistic Cyber Warfare Exercises
- Intelligent Software Decoy Tools for Cyber
- MIL-STD-1553B protocol covert channel analysis
- Making Sense of Email Addresses on Drives
- Modeling Cyber-Physical War-Gaming
- NEXT GENERATION REPOSITORY FOR SHARING SENSITIVE NETWORK AND SECURITY DATA
- Network-Enabled Operations - Social Network Analysis of Information Sharing
- RussiaтАЩs Approach to Cyber Warfare
- Trusted Computer Exemplar -Physical Security Plan
- Trusted Computing Exemplar -Configuration Management Procedures

Contact Us

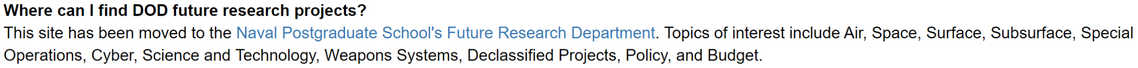
Information Desk
☎ (831) 656-2947
✉ circdesk@nps.edu
Floor Map

You might also be interested in...

- Borrowing Privileges by User Type
- My Interlibrary Loan Account
- Interlibrary Loan Policies
- Course Reserves Policies

Figure 5. Screenshot of the cyber-topic subpage and related downloadable PDF documents.

To help increase honeypot traffic, we also added links from legitimate Naval Postgraduate School webpages that redirected users to the honeypot website. We placed the links in locations that would be found only by someone scraping the official library and faculty webpages. We put links on Dr. Rowe's faculty page (http://faculty.nps.edu/ncrowe/) and on the library webpages titled "My Navy Portal" (https://libguides.nps.edu/portals/NKO), (Figure 6), and on "Military Rank, Insignia, Awards, Seals, Ceremonies" (http://libguides.nps.edu/militaryrank/MilitaryBadges).



Where can I find DOD future research projects?

This site has been moved to the Naval Postgraduate School's Future Research Department. Topics of interest include Air, Space, Surface, Subsurface, Special Operations, Cyber, Science and Technology, Weapons Systems, Declassified Projects, Policy, and Budget.

Figure 6. Screenshot of link to honeypot website from the NPS library "My Navy Portal" webpage.

B. TRAFFIC DATA COLLECTION

We used Google Analytics and AWStats to track and record interactions with our honeypot website. Google Analytics is a popular free web-analytics software suite that tracks website usage. It provides information on which pages users interact with the most, how long they spend on each page, from what page the user found the website, and general user geographic information. Google Analytics does not collect any personally identifiable information and strips the user's IP address. Google Analytics presents the data as statistics to identify trends and patterns with website interaction. We added a Tracking ID to the honeypot homepage and subpage HTML files to enable the Google Analytics server to log interaction with it. Additionally, we created an event trigger to record each time one of our PDF files was downloaded so that we could analyze which were the most popular. Note that Google Analytics attempts to exclude Internet bot traffic to help website administrators focus on actual user interaction.

In addition to Google Analytics, we used AWStats to analyze honeypot interactions and file downloads. AWStats is a free analytic tool that assists website administrators in examining webserver-generated log files to determine the number of website visitors, visit duration, most viewed pages and files, HTTP errors, and general user geographic information. Because AWStats pulls data from the webserver logs, it does not distinguish human users from bots. Additionally, AWStats cannot fuse different statistical data sets like Google Analytics can. For example, Google Analytics could provide statistics regarding which file was the most popular among users of a certain country, whereas AWStats could provide only the file that was the most popular and which country accessed the website the most.

C. A WEBSITE SURVEY

To supplement our honeypot collection, we conducted a survey with Naval Postgraduate School students and members of the general public. We wanted to ask directly how real users perceived our honeypot website and which categories and files attracted their attention. Specifically, we wanted to collect data on user interaction to determine if users viewed our honeypot as a legitimate Naval Postgraduate School resource, and on what they would focus their collection efforts if they were tasked to collect intelligence on a Department of Defense institution. We did not inform survey participants of the honeypot website's true nature and we asked the following questions (Appendix C) while they interacted with the honeypot website:

- Would you assume that the Naval Postgraduate School (NPS) owns and maintains this website?
- What details or characteristics make you think that the site is or is not a legitimate NPS resource?
- If you are unsure of the website's legitimacy, is it compelling enough for you to continue exploring and browsing the webpage and subpages?
- Which categories seem most interesting or most important?
- If you were tasked with collecting information on the United States Department of Defense and you found this website, in which category would you focus your collection efforts?
- Are there any specific documents that appear particularly compelling?

We chose a mixture of Naval Postgraduate School students and members of the general public because students are more likely to view and interact with legitimate library webpages while members of the general public may not have seen a Naval Postgraduate School website. We wanted to test how users within the school viewed the honeypot differently.

V. DATA AND RESULTS

From 20 April 2018 to 30 September 2018, Google Analytics reported 781 pageviews from 107 visitors and AWStats reported 14,760 pageviews from 6,718 visitors to our site. The large difference in reported activity is due to exclusion of bot traffic from the statistics reported by Google Analytics. AWStats reports more traffic, but does not characterize user interactions in as much detail. Assuming that Google Analytics captured all human interaction with the web server, we estimate that bots were responsible for 98.38 percent of all traffic on our site.

A. DATA COLLECTION AND ANALYSIS

Within six weeks of activating our honeypot website, our search-engine queries for “nps future research” moved from the fifth page of results to the top result in Google queries. On average, our honeypot’s traffic increased during the initial collection period and reached the height of activity during June and July, as shown in Figures 7–9. In September, we conducted user surveys and asked participants to access our site and provide feedback, which increased September’s number of users, pageviews, and downloads. Participants were typically asked to conduct a Google query for “nps future research” and our honeypot website was consistently a top result.

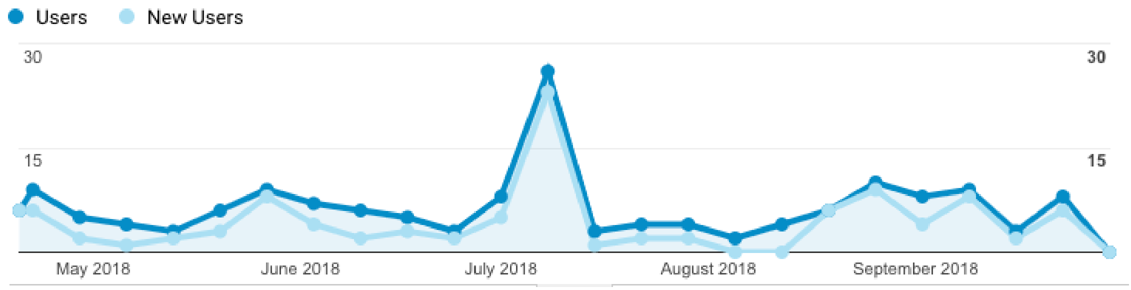


Figure 7. Google Analytics—Users over time.

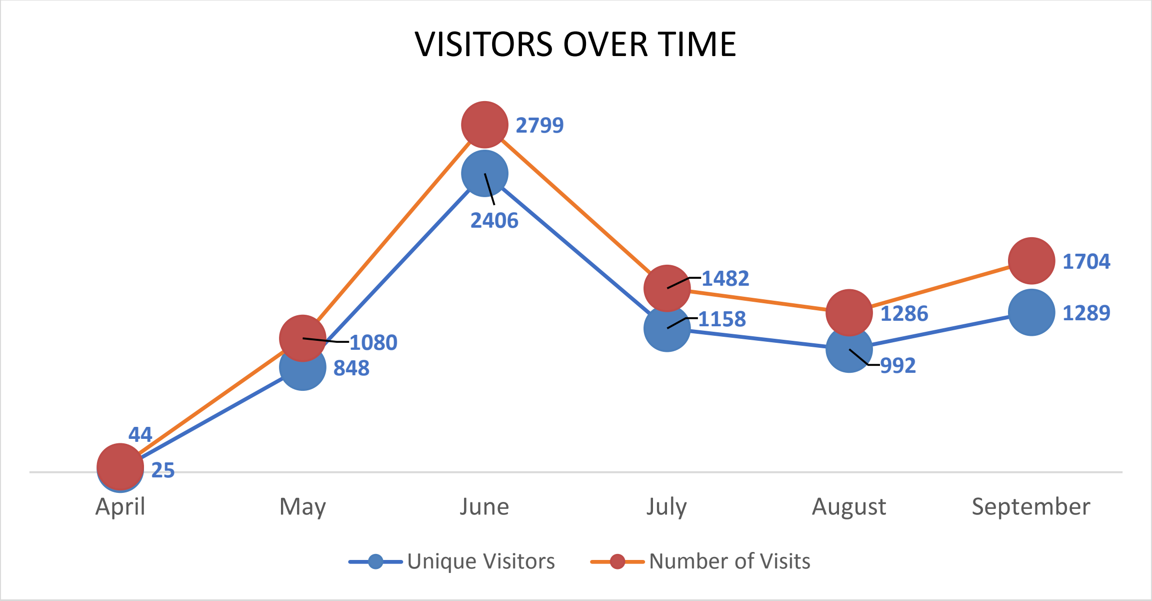


Figure 8. AWStats—Visitors over time.

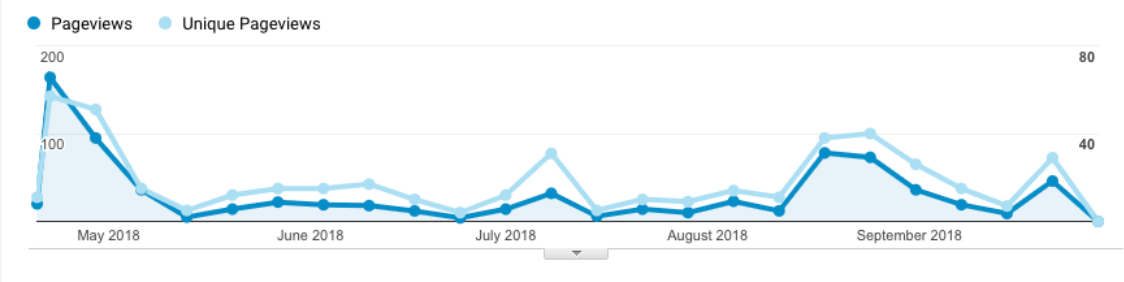


Figure 9. Google Analytics—Pageviews over time.

Google Analytics showed a spike in activity during July while AWStats showed a peak of activity in June before returning to similar levels of activity in May. According to both analytic tools, the number of new or unique visitors tracked slightly below the path of total visits and total users.

Google Analytics only counts pageviews on pages that have been labeled with the Analytics code in the HTML file. If a user refreshes the tracked page, or visits a different page and then revisits the tracked page, it is counted as an additional pageview (Google Analytics, 2018). However, Google Analytics defines unique pageviews as “the number of sessions during which that page was viewed one or more times” (Google Analytics, 2018).

Thus, if a user refreshes the page multiple times or visits other pages and then returns to the tracked page, it is counted as one unique pageview. We would expect pageviews to be higher than unique pageviews because a single user could generate multiple pageviews during a session, but our data consistently shows unique pageviews being higher than pageviews. Figure 9 shows a spike in pageviews and unique pageviews in July, which is consistent with the peak in the number of users. However, May and September had even more pageviews when user level experienced moderate peaks.

AWStats defines "pages" as the number of pages that visitors view, where pages are typically HTML, PHP, or ASP files (Destailleur, n.d.). AWStats defines "hits" as any file requested from the server. Because a user can view multiple pages, the number of pages and hits is significantly higher than the number of users. Nonetheless, the visitors-over-time (Figure 8) graph closely resembled the pages-over-time graph (Figure 10). The data suggests that our honeypot reached a peak level of interest during weeks 8 through 12 of the experiment, with user interaction leveling out in the following months.

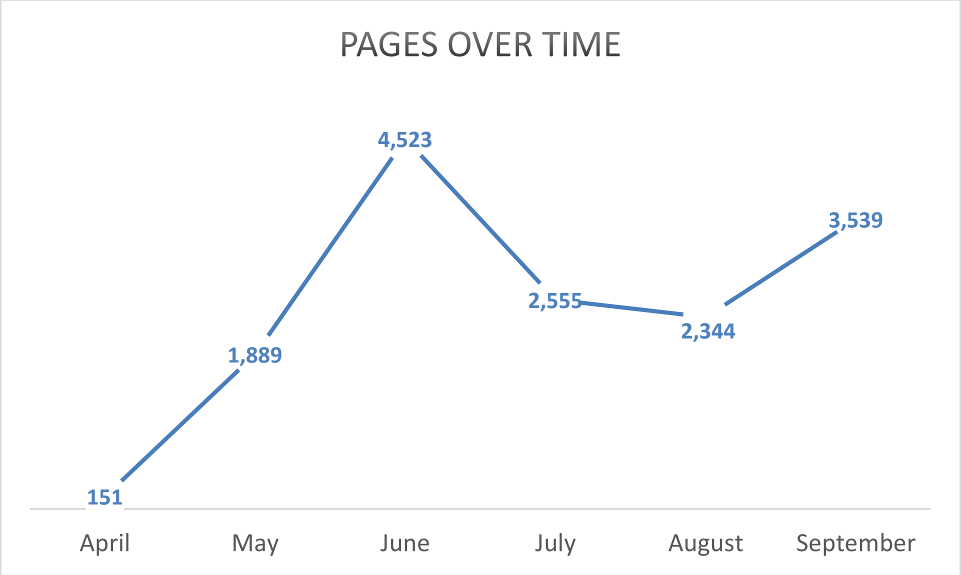


Figure 10. AWStats—Pages over time.

Figure 11 shows the overall level of activity reported by AWStats over time. Dips in the graph that indicate no visits, pages, or hits represent periods when our server was off. We shut down our server from 27 July–02 Aug 2018 for administrative purposes, and a power outage caused a shutdown from 12–14 Aug 2018. These shutdowns contributed to lower overall activity in July and August compared to June and September.

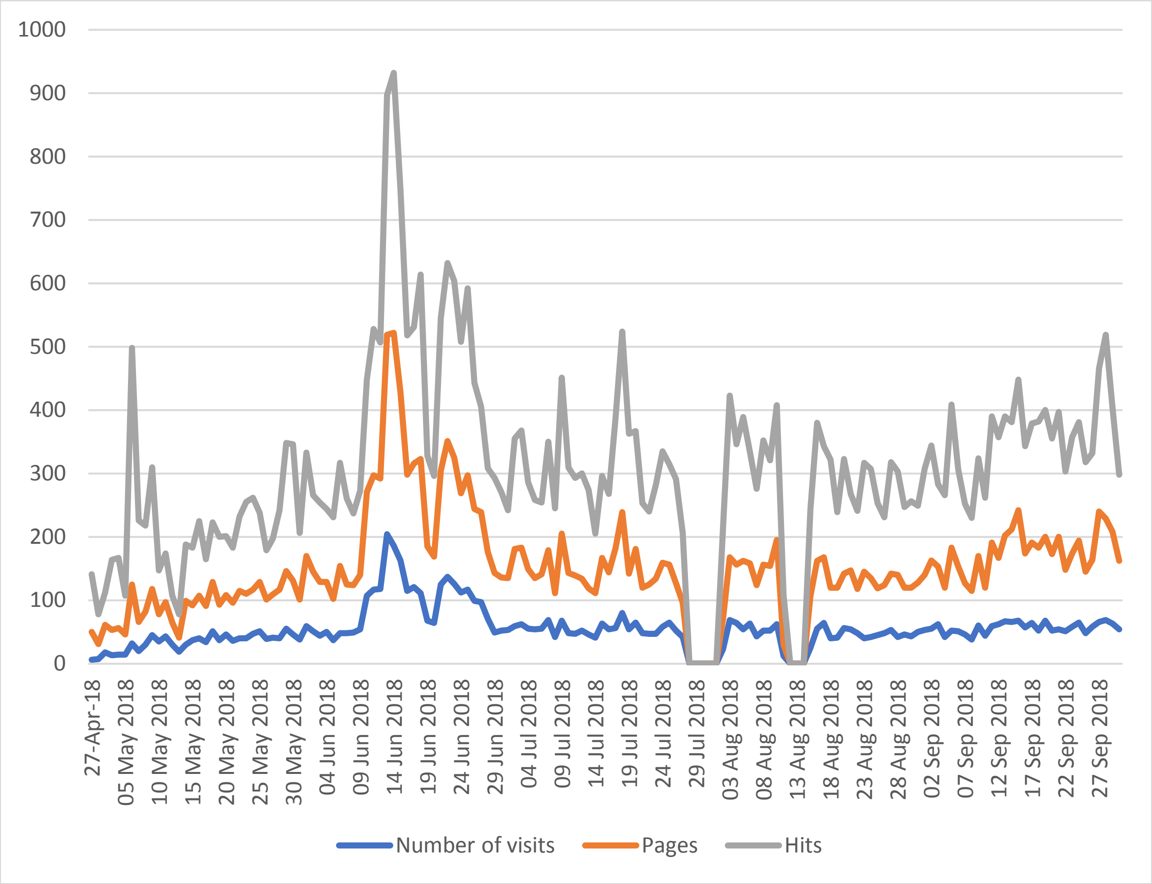
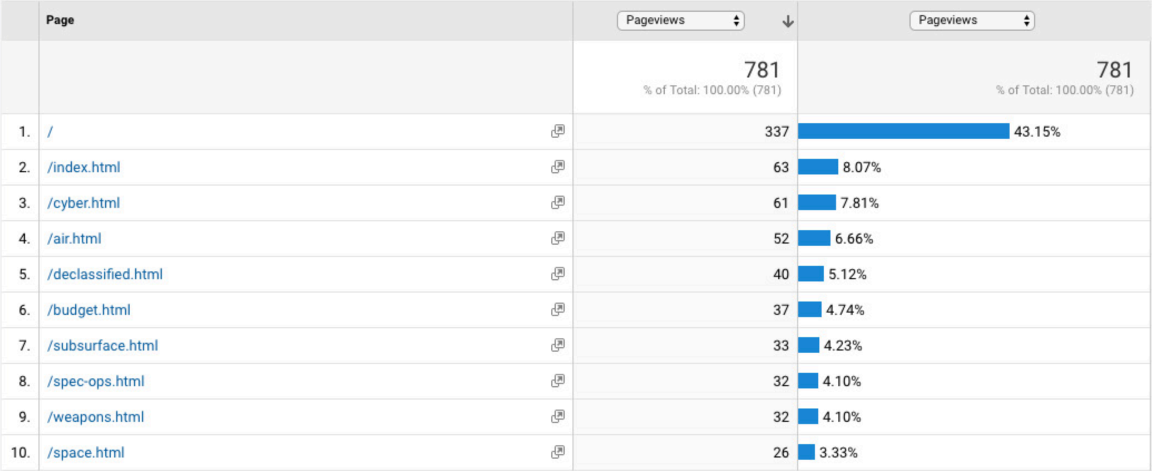


Figure 11. AWStats—Visits, pages, and hits over time.

1. Popularity of Documents

Google Analytics showed that the honeypot website homepage, represented by "/" and "/index.html" in Figure 12, was the most commonly visited page, having 51.22 percent of total pageviews. This is expected as most users enter the website via the homepage. Google Analytics reported that the cyber page was the most commonly viewed category page, followed by air and declassified projects. Note that cyber is not listed first on the home page. These results included participant surveys conducted during September. We estimate that these surveys contributed to an additional 34 users and 150 pageviews. Survey participants rarely downloaded files; they made selections based on title alone. We assess the that number of survey participant file downloads was negligible.



	Page	Pageviews	Pageviews
		781 % of Total: 100.00% (781)	781 % of Total: 100.00% (781)
1.	/	337	43.15%
2.	/index.html	63	8.07%
3.	/cyber.html	61	7.81%
4.	/air.html	52	6.66%
5.	/declassified.html	40	5.12%
6.	/budget.html	37	4.74%
7.	/subsurface.html	33	4.23%
8.	/spec-ops.html	32	4.10%
9.	/weapons.html	32	4.10%
10.	/space.html	26	3.33%

Figure 12. Google Analytics—Most visited pages.

Compiled AWStats logs show that the home page represented 91.13 percent of page views, with cyber as the most commonly viewed category with .085 percent of all pageviews. The pageview results from AWStats are shown in Table 1. The AWStats logs show cyber as the most commonly viewed subpage, followed by air and declassified projects. This is consistent with the top three pages as reported by Google Analytics. Budget, surface, and policy were the least viewed subpages, with 0.69 percent each of total pageviews.

Table 1. AWStats—Summary of pageviews.

Pages	Sum of Viewed	Percentage Viewed
homepage	13451	91.13%
/cyber.html	126	0.85%
/air.html	118	0.80%
/declassified.html	115	0.78%
/space.html	114	0.77%
/weapons.html	113	0.77%
/subsurface.html	112	0.76%
/science-tech.html	111	0.75%
/spec-ops.html	107	0.72%
/budget.html	102	0.69%
/surface.html	102	0.69%
/policy.html	102	0.69%
http://www.ip.cn/	14	0.09%
http://httpheader.net/	14	0.09%
http://www.minghui.org/	13	0.09%
http://www.123cha.com/	13	0.09%
http://www.wujieliulan.com/	11	0.07%
http://www.epochtimes.com/	11	0.07%
http://boxun.com/	11	0.07%
Grand Total	14760	100.00%

The bottom of Table 1 shows pageviews to seven different pages that we did not host on the webserver. These were proxy requests to Chinese websites, but AWStats counts them as pageviews because the Apache webserver sent a 200-success status code to the client. We disabled proxying on our webserver, but RFC2616 section 5.1.2 mandates that "Apache must accept requests with absolute URLs in the request-URI, even for non-proxy requests" (Apache, 2012). Apache documentation states that Apache will continue to accept proxy requests even if proxying is disabled. However, instead of serving the external site's content, Apache delivered our site's content at the corresponding location on our webserver, which we defined as the default homepage.

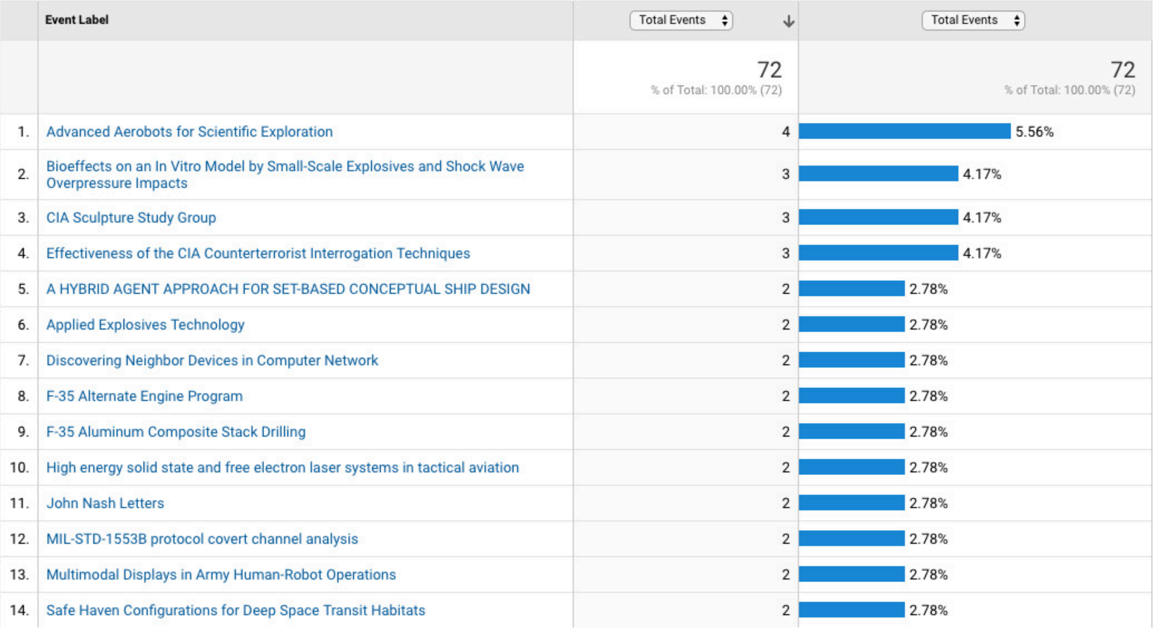
Table 2 shows the breakdown of pageviews by category, excluding the homepage and proxy requests. Cyber was the most commonly viewed subpage, but less than one percent difference separated the top four most-viewed subpages. The top three most-viewed subpages reported through AWStats are consistent with the top three reported through Google Analytics.

Table 2. AWStats—Summary of hosted category pageviews.

Pages	Sum of Viewed	Percent Viewed
/cyber.html	126	10.31%
/air.html	118	9.66%
/declassified.html	115	9.41%
/space.html	114	9.33%
/weapons.html	113	9.25%
/subsurface.html	112	9.17%
/science-tech.html	111	9.08%
/spec-ops.html	107	8.76%
/budget.html	102	8.35%
/surface.html	102	8.35%
/policy.html	102	8.35%
	1222	100.00%

2. Popular Documents

We tracked file downloads through Google Analytics and AWStats to see which documents were downloaded the most. Google Analytics did not show the same level of document downloads as AWStats, but both collection mechanisms provided insights into user interests. Figure 13 shows the documents tracked by Google Analytics that were downloaded at least twice. Of the 132 hosted documents, Google Analytics reported that users downloaded 72 different documents. Fourteen documents were downloaded more than once.



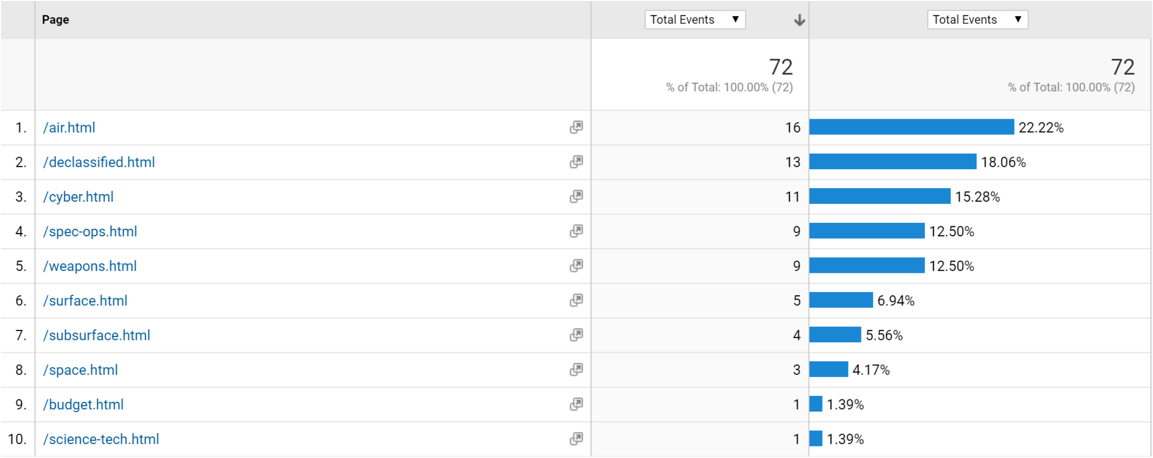
	Event Label	Total Events	Total Events
		72 % of Total: 100.00% (72)	72 % of Total: 100.00% (72)
1.	Advanced Aerobots for Scientific Exploration	4	5.56%
2.	Bioeffects on an In Vitro Model by Small-Scale Explosives and Shock Wave Overpressure Impacts	3	4.17%
3.	CIA Sculpture Study Group	3	4.17%
4.	Effectiveness of the CIA Counterterrorist Interrogation Techniques	3	4.17%
5.	A HYBRID AGENT APPROACH FOR SET-BASED CONCEPTUAL SHIP DESIGN	2	2.78%
6.	Applied Explosives Technology	2	2.78%
7.	Discovering Neighbor Devices in Computer Network	2	2.78%
8.	F-35 Alternate Engine Program	2	2.78%
9.	F-35 Aluminum Composite Stack Drilling	2	2.78%
10.	High energy solid state and free electron laser systems in tactical aviation	2	2.78%
11.	John Nash Letters	2	2.78%
12.	MIL-STD-1553B protocol covert channel analysis	2	2.78%
13.	Multimodal Displays in Army Human-Robot Operations	2	2.78%
14.	Safe Haven Configurations for Deep Space Transit Habitats	2	2.78%

Figure 13. Google Analytics—Most downloaded documents.

Google Analytics reported that users downloaded the aerobots document the most with 5.56 percent of all downloads. We suspect that this is due to the document categories being listed alphabetically, with the air category first, and the aerobots document was the first listed on the air subpage. This suggests that human users tend to access pages and documents in order and incompletely.

However, we did not see any evidence that bots were accessing pages or downloading documents in order or alphabetically. AWStats, which mainly reported bots, showed that the budget category had among the lowest number of pageviews and document downloads, but it was presented second after the air category. Additionally, we did not find any evidence that the most recently published documents were downloaded more frequently. The most frequent document download reported by AWStats was for a document published in 2018, but the second and third most downloaded documents were published in 2010 and 2014, respectively. Additionally, some documents that were published within the last year had few downloads.

Figure 14 shows the categories of the most downloaded documents as reported by Google Analytics. The air subpage had the most downloaded documents, consisting of 22.22 percent of all downloads, followed by declassified projects and cyber. These top three categories of document downloads were the same as the top three subpage pageviews but in a different order.



	Page	Total Events ▼	Total Events ▼
		72 % of Total: 100.00% (72)	72 % of Total: 100.00% (72)
1.	/air.html	16	22.22%
2.	/declassified.html	13	18.06%
3.	/cyber.html	11	15.28%
4.	/spec-ops.html	9	12.50%
5.	/weapons.html	9	12.50%
6.	/surface.html	5	6.94%
7.	/subsurface.html	4	5.56%
8.	/space.html	3	4.17%
9.	/budget.html	1	1.39%
10.	/science-tech.html	1	1.39%

Figure 14. Google Analytics—Categories of most downloaded documents.

AWStats reported that the neural network paper from the science & technology category was the most downloaded document with 591 downloads. This document had over 2.5 times as many downloads as the reported second most downloaded document. Of note, this document was downloaded 489 times and partially downloaded 169 times during the month of July, but during the rest of the months it averaged 20.4 downloads per month. The top ten downloaded documents as reported by AWStats are shown in Table 3 and Figure 15. Table 3 shows the number of downloads and partial downloads. The Mars vehicle document from the space category had 462 partial downloads and only 30 downloads. One document in the surface category and one in the policy category also had partial downloads in the 400’s, but had about three times as many complete downloads.

Table 3. AWStats—Top 10 downloads.

Category	Top 10 Downloads	Sum of Hits	Sum of 206 Hits
Science & Technology	Multi-Task Convolutional Neural Network for Pose-Invariant Face Recognition	591	328
Surface	Hydrostatic and hydrodynamic analysis of a lengthened DDG-51	207	104
Surface	DDG-1000 missile integration	182	211
Policy	China’s evolving foreign policy in Africa	149	10
Surface	Establishing the Fundamentals of a Surface Ship Survivability Design Discipline	130	220
Special Operations	Roles of Perseverance, Cognitive Ability, and Pysical Fitness - U.S. Army Special Forces	128	19
Surface	A Salvo Model of Warships in Missile Combat Used to Evaluate Staying Power	110	411
Cyber	MIL-STD-1553B protocol covert channel analysis	109	72
Policy	Analysis of government policies to support sustainable domestic defense industries	92	16
Policy	Russia’s natural gas policy toward Northeast Asia	89	421

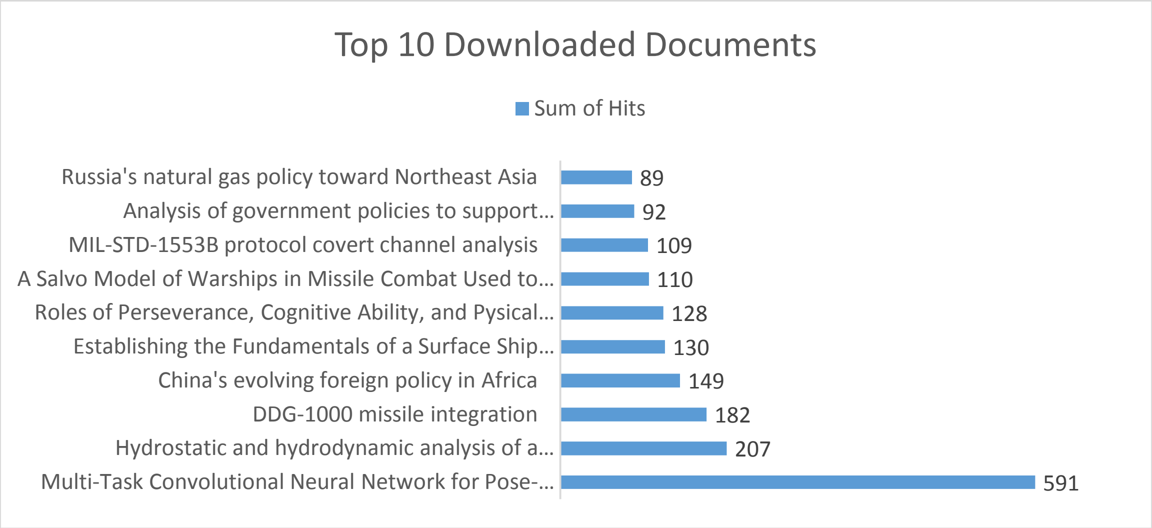


Figure 15. AWStats—Top 10 downloaded documents.

Overall, the science & technology category had the most document downloads, followed by the surface category. This is counter to what we saw with AWStats in which science & technology and surface pages were 7th and 10th, respectively. Additionally, Google Analytics reported that science & technology had only one download. A summary of document downloads by category is shown in Figure 16 and Table 4.

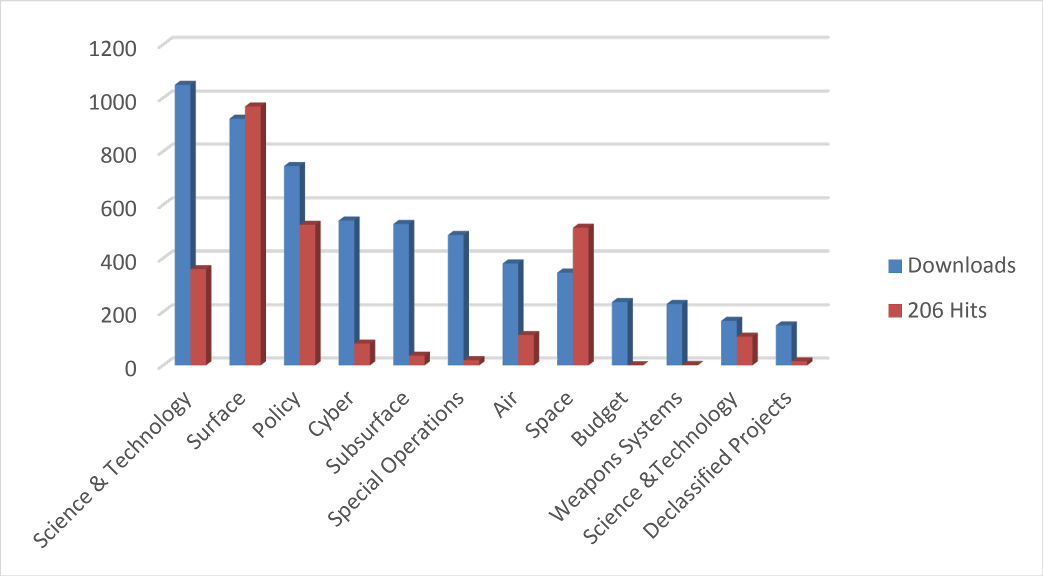


Figure 16. AWStats—Total downloads by category.

Figure 16 and Table 4 show the number of downloads by category and the number of partial downloads in which users stopped the download before completion. Because we were not using commercial-grade server hardware, users may have experienced longer-than-normal download times that made full-document downloads more difficult.

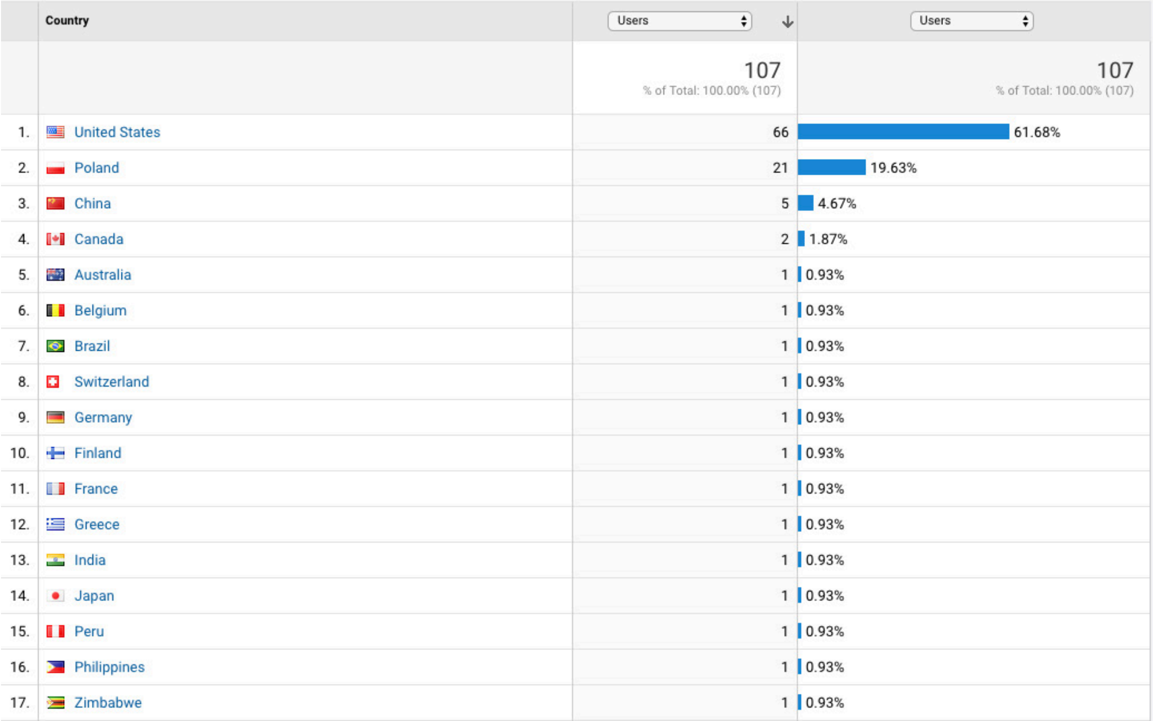
Table 4. AWStats—Total downloads by category.

Category	Downloads	206 Hits
Science & Technology	1049	359
Surface	922	968
Policy	745	525
Cyber	541	81
Subsurface	528	36
Special Operations	487	19
Air	380	113
Space	346	514
Budget	236	0
Weapons Systems	229	1
Science &Technology	166	107
Declassified Projects	149	15
Grand Total	5778	2738

Several document download counts exceeded the number of page hits for that category. For example, the most popular document about neural networks under the science & technology category and was fully downloaded 591 times and partially 328 times. However, science & technology had only 111 pageviews reported by AWStats. We infer that bots are downloading the same document multiple times after their initial pageview and that bots directly accessing the document links circumvent the category page count.

3. Activity by Country

We analyzed activity by users' countries through both Google Analytics and AWStats, although IP addresses can be spoofed and requests can be purposely obfuscated through proxies. Figure 17 shows Google Analytics' characterization of all 107 users. The United States led the visiting countries with 61.68 percent of users and Poland was second with 19.63 percent. Additionally, Google Analytics reported 13 countries with only one visitor. If the same user has multiple visits to a site, the visitor count remains unchanged but the pageviews increase.



	Country	Users	Users
		107 % of Total: 100.00% (107)	107 % of Total: 100.00% (107)
1.	United States	66	61.68%
2.	Poland	21	19.63%
3.	China	5	4.67%
4.	Canada	2	1.87%
5.	Australia	1	0.93%
6.	Belgium	1	0.93%
7.	Brazil	1	0.93%
8.	Switzerland	1	0.93%
9.	Germany	1	0.93%
10.	Finland	1	0.93%
11.	France	1	0.93%
12.	Greece	1	0.93%
13.	India	1	0.93%
14.	Japan	1	0.93%
15.	Peru	1	0.93%
16.	Philippines	1	0.93%
17.	Zimbabwe	1	0.93%

Figure 17. Google Analytics—All visitors by country.

AWStats allowed for further analysis of user locations in the Apache server logs. We used the free online IP/DNS lookup tool InfoByIP.com to match user IP and domain names to countries. It could not characterize all IPs, so we supplemented our analysis with the Linux "whois" tool and the online tools AbuseIPDB and MYIP.MS. For domain names that the lookup tools could not geolocate, we used the domain name's country code suffix to assign the country. During June, July, and September the honeypot had more than 1,000 unique users per month, but configuration settings in AWStats limited analysis to 1,000.

Through the AWStats logs, we identified user requests from 138 countries. The United States was the leading user country with 16.12 percent and Brazil was second with 15.01 percent. China and Russia were third and fourth with 7.19 and 6.29 percent, respectively. Figure 18 shows the disposition of the top ten countries by unique visitor where percentages are among the top ten countries. Table 5 shows the actual counts.

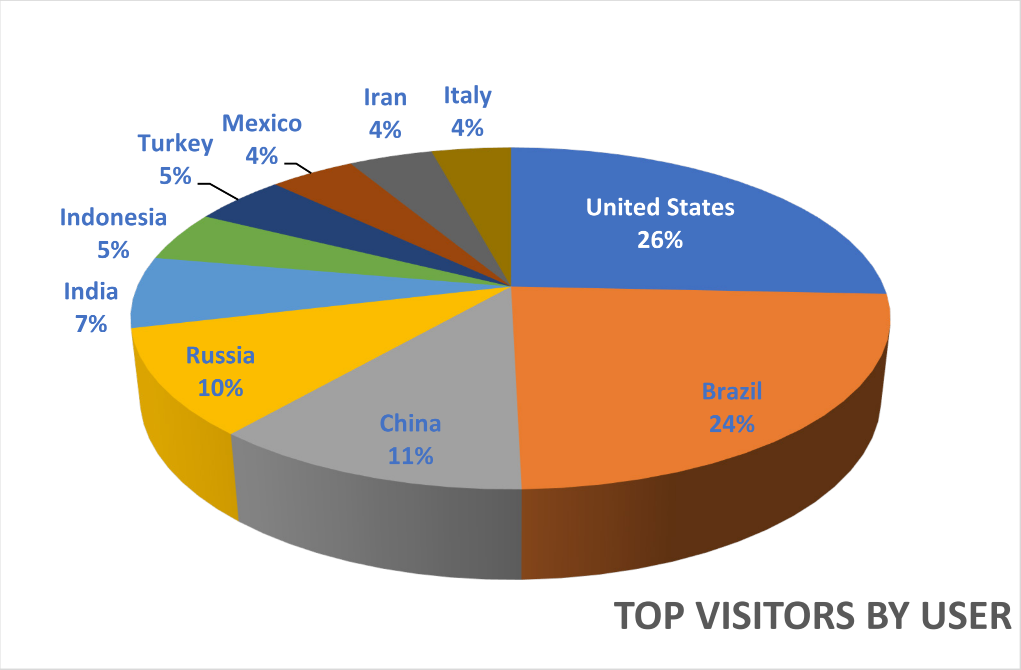


Figure 18. AWStats—Top 10 visiting countries by unique visitor.

Table 5. AWStats—Top 10 visiting countries by user.

Country	Users per Country
United States	800
Brazil	745
China	357
Russia	312
India	210
Indonesia	148
Turkey	147
Mexico	135
Iran	133
Italy	126

We also arranged countries by number of pageviews to account for some users visiting the honeypot multiple times. Users from the United States accounted for 42.13 percent of all page visits, with Brazil in second with 8.12 percent. Russian and Chinese users accounted for the third and fourth most common visitors with 6.38 and 5.85 percent of all page visits, respectively. Figure 19 shows the disposition of the top ten countries by pageviews, and Table 6 shows the counts.

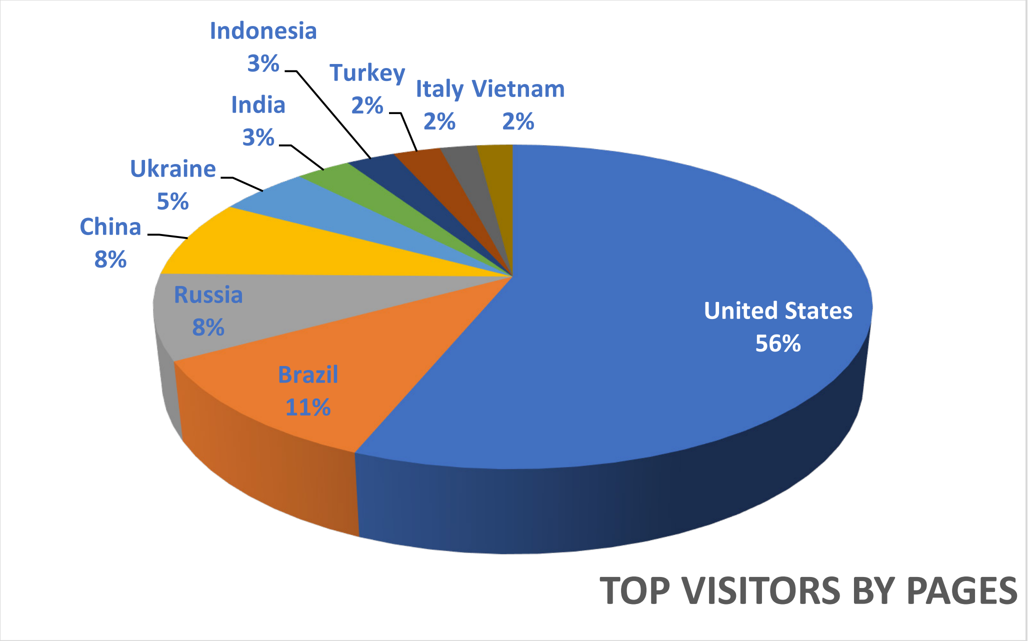


Figure 19. AWStats—Percentages of top 10 visiting countries by page views.

Table 6. AWStats—Top 10 visiting countries by page views.

Country	Sum of Page views
United States	5539
Brazil	1067
Russia	839
China	769
Ukraine	482
India	292
Indonesia	259
Turkey	252
Italy	196
Vietnam	192

4. User Surveys

To get a better understanding of our honeypot webpage effectiveness, we surveyed 25 Naval Postgraduate School students and 9 members of the general public. Naval Postgraduate School students likely interact with the school and library website on a regular basis and may notice inconsistencies with our honeypot website compared to the legitimate websites. However, members of the general public typically have never seen or interacted with the school or library webpages

Sixty-four percent of Naval Postgraduate School Students and one hundred percent of members of the general public stated that they assumed the Naval Postgraduate School owned and maintained the honeypot website. Of the participants, only three students stated that the website did not appear compelling enough for them to continue exploring. Of the students who did not think the honeypot was legitimate, they noted it had a URL ending in .org instead of .edu like all other Naval Postgraduate School websites, and it lacked a "secure" logo that accompanies https websites. Of those who assumed the website's legitimacy, respondents stated that the layout, header and footer, contact information, banner, functioning school links, and Google and Facebook plugins led them to believe that the Naval Postgraduate School maintained the website.

We asked participants to select the categories of documents that seemed most interesting or most important. Participants were not required to pick only one category, so the number of responses was greater than the number of those surveyed. Student results are shown in Table 7 and general public responses are shown in Table 8. One student respondent stated that none of the categories appeared interesting or important.

Table 7. NPS student responses to most interesting or most important categories.

Category	Count of Responses
Cyber	17
Declassified Projects	11
Science & Technology	10
Special Operations	9
Weapons Systems	9
Space	8
Policy	4
Subsurface	3
Budget	1
None	1
Air	1
Surface	1
Grand Total	**75**

Table 8. General public responses to most interesting or most important categories.

Category	Count of Responses
Cyber	6
Special Operations	5
Weapons Systems	4
Space	3
Declassified Projects	2
Science & Technology	2
Air	1
Budget	1
Surface	1
Grand Total	**25**

We asked participants to choose the categories in which they would focus their collection efforts if they were tasked with collecting information on the United States Department of Defense. We asked this question to gain insight into what types of documents that participants thought foreign intelligence would be interested in collecting. Participants often chose multiple categories; their responses are summarized in Table 9 and 10. Three respondents stated that they would focus their collection efforts in all categories.

Table 9. NPS student responses to possible categories of interest by foreign intelligence.

Category	Count of Responses
Weapons Systems	17
Cyber	16
Science & Technology	12
Special Operations	10
Declassified Projects	9
Space	9
Budget	4
Subsurface	4
Policy	3
All	2
Air	2
Surface	1
Grand Total	**89**

Table 10. General public responses to possible categories of interest by foreign intelligence.

Category	Count of Responses
Cyber	5
Weapons Systems	4
Special Operations	3
Declassified	3
Science & Technology	2
Surface	1
All	1
Policy	1
Budget	1
Subsurface	1
Grand Total	**22**

We asked participants if any documents appeared particularly compelling. Cyber was the most popular category among all respondents (Tables 11 and 12). The data repository document from the cyber category was selected a total of eight times, making it the most popular among respondents. Two other documents were selected a total of six times, the Russian cyber warfare document and the software decoy document, both listed under the cyber category.

Table 11. NPS student compelling documents by category.

Category	Count of Documents by Category
Cyber	26
Subsurface	9
Weapons Systems	9
Science & Technology	5
Air	3
Declassified	3
Space	2
All	1
Policy	1
Special Operations	1
Grand Total	**60**

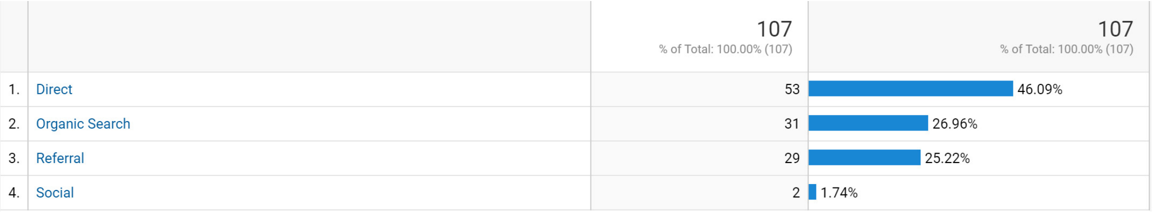
Table 12. General public compelling documents by category.

Category	Count of Documents by Category
Cyber	10
Special Operations	7
Weapons Systems	3
Budget	1
Grand Total	**21**

Participants consistently chose cyber as a most important category and chose documents from the cyber category more than twice as often as any other document category. This is consistent with it being the top pageview category reported by Google Analytics and AWStats.

5. Website Access

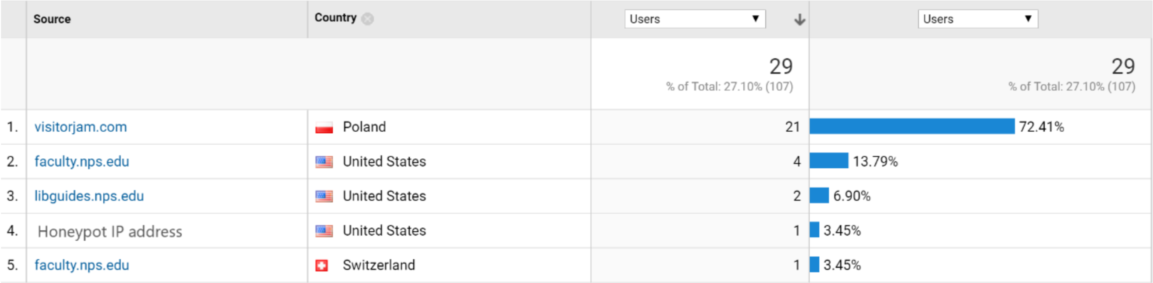
Using Google Analytics, we tracked how users reached our website (Figure 20). Because Google Analytics typically excludes bot traffic, our results likely summarize the activity of human users. (We were unable to collect information regarding site referrals with AWStats.) Direct access was the most common method, meaning that users went directly to the website without using a search engine. Organic search, the second most common method, means users that found our website with a search engine. Referral means that other websites referred traffic to our site through a link. Social indicates that our site was found via social media. Both social media referrals were from Facebook.



		107 % of Total: 100.00% (107)	107 % of Total: 100.00% (107)
1.	Direct	53	46.09%
2.	Organic Search	31	26.96%
3.	Referral	29	25.22%
4.	Social	2	1.74%

Figure 20. Google Analytics—User access to honeypot website.

The referral sites are shown in Figure 21. Twenty-one users from Poland accessed our honeypot through the site visitorjam.com which is unaffiliated with the Naval Postgraduate School or our research. A "whois" lookup indicated that visitorjam.com is registered in Australia. Four users from the United States and one user from Switzerland accessed our website through a link on Prof. Rowe's faculty page, indicated by "faculty.nps.edu" in Figure 21. Two users found our website through the links placed on library pages as described earlier. Lastly, one user accessed our honeypot directly through its IP address. For safety, we removed the actual IP address of our honeypot from Figure 21 line 4.



	Source	Country	Users ▼ ↓	Users ▼
			29 % of Total: 27.10% (107)	29 % of Total: 27.10% (107)
1.	visitorjam.com	Poland	21	72.41%
2.	faculty.nps.edu	United States	4	13.79%
3.	libguides.nps.edu	United States	2	6.90%
4.	Honeypot IP address	United States	1	3.45%
5.	faculty.nps.edu	Switzerland	1	3.45%

Figure 21. Google Analytics—Summary of referring websites.

B. DATA COLLECTION CHALLENGES AND EVALUATION

We initially intended to only use Google Analytics to monitor Web traffic, but we realized that its bot exclusions limited useful data considerably. We then decided to use AWStats as a secondary collection method. If users disable cookies or JavaScript from their Web browsers, Google Analytics may not count their visits (UltimateWB, 2014), but this is rare. Attracting more human users would have added value to our experimentation.

When we installed AWStats, we did not realize that the default in the configuration file limited the number of rows displayed to 1,000. In some months our honeypot had more than 1,000 users, so we could not perform geolocation analysis on all since AWStats would only list them as "other" visitors. We modified the configuration file to display up to 5,000 rows, but the change did not apply retroactively.

Google Analytics displayed user geographic information for all reported users, but AWStats was not always successful at identifying user locations. We used online tools for bulk IP address lookups, but we still had to manually investigate hundreds of IP address and domain names that were not properly identified. A more capable automated system could have saved many hours of analysis.

During our experiments, our server was powered off for more than eight full days: five days for administrative issues, and three days due to a power outage. Better warning by the School administrative departments and an uninterruptable power supply could have aided data collection. Additionally, the hardware that we used for the server was volatile and would often disconnect from the Internet after software updates or power cycles. On several occasions the server was down for a few hours while we troubleshot connectivity issues. These power and connectivity issues may have tipped off astute, frequent honeypot visitors to our website's legitimacy.

VI. CONCLUSIONS

A. FINDINGS

Web-based honeypots can effectively identify areas of interest to Internet users. Pageviews and file downloads on our honeypot showed specific user interests which may help identify priorities regarding broader Internet data theft. The Google Analytics data collection mainly represented human users while the AWStats collection mostly represented bots, but both tools reported pageviews that indicated a primary interest in the cyber, air, and declassified projects categories. Survey respondents also indicated cyber as their most popular category.

Interestingly, the most popular file downloads did not always coincide with the most commonly viewed pages. Google Analytics reported that air, declassified projects, and cyber had the most downloaded documents while AWStats indicated that science & technology, surface, and policy had the most downloads. The differences are likely due to human-user behavior versus bot-user behavior. We noted that human users may have accessed documents in the air category because it was presented first on the webpage. Numerous downloads of the same document during some months may indicate flaws in bot search algorithms causing repeated downloads, or perhaps time-sensitive trends in bot data collection.

Our data showed that users accessed our honeypot website from 138 different countries, with the United States as the most common and Brazil as second. While the IP address does not provide a definitive user geolocation, it offers insight into trends and possible pivot points for users trying to obscure their true location. IP address trends can provide useful traffic filtering data for legitimate information systems. Our honeypot provided insight into these trends without harming Department-of-Defense interests.

We anticipated seeing more human-user interaction in our data, but manual data collection may be rare like many other manual processes in the cyber realm. Studying both human and bot activity will increase cyber security by understanding how and why each operates in cyberspace.

B. FUTURE RESEARCH

Identifying trends among bots and how they identify and download documents would provide valuable insight into Internet-based intelligence collection. It is unlikely that bots indiscriminately download documents. Further research into this area would add value to overall cyber security as cyber attacks and intelligence collection move towards more automated processes. Additionally, monitoring individual or associated bots over time while tracking document downloads could provide useful information about specific interests of an organization.

Studying user interaction with a Web-based honeypot through tracking of mouse activity could provide additional information into user interests. By studying where users move and hover the mouse on a web-based honeypot may indicate areas of interest or disinterest. A mouse that hovers over an area without clicking the links may suggest that the user investigated a category but decided not to explore it further. Bots are unlikely to have any mouse movements so that would help identify them. Additionally, studying the duration of time between clicks on a honeypot could help discern a human-user versus a bot-user. Humans require time for reading between clicks, so slower click frequencies would likely indicate a human user.

APPENDIX A. HONEYPOT DOCUMENT TITLES

AIR

File Name
Advanced Aerobots for Scientific Exploration
Artificial Intelligence Based Control Power Optimization on Tailless Aircraft
Command and control models of next generation unmanned aircraft systems
Design Process of Flight Vehicle Structures for a Common Bulkhead and an MPCV Spacecraft Adapter
F-35 Alternate Engine Program
F-35 Aluminum Composite Stack Drilling
Flight Vehicle Structural Design Processes for a Common Bulkhead and a Multipurpose Crew Vehicle Spacecraft Adapter
High energy solid state and free electron laser systems in tactical aviation
Investigation of Missile Control Surface Effects on F-16 Limit-Cycle Oscillation
Subsonic Ultra Green Aircraft Research - Hybrid Electric Design Exploration
UAV Supervisory Control on F-18 Formation Flight Performance

BUDGET

File Name
America First - A Budget Blueprint to Make America Great Again
An Update to the Budget and Economic Outlook - 2017 to 2027
Cash and Accrual Measures in Federal Budgeting
Counter-ISIS Train and Equip Fund
DARPA Funds Surprising Systems
Federal Debt and the Statutory Limit, January 2018
Inflation and Price Escalation Adustments - F-35
Long-Range Plan for Construction of Naval Vessels for Fiscal Year 2019
Military Personnel Programs
Options for Reducing the Deficit - 2017 to 2026
Program Acquisition Cost by Weapon System
Research Development, Test & Evaluation Programs
The Acceptability of War and Support for Defense Spending
The Depot-Level Maintenance of DoD's Combat Aircraft - Insights for the F-35

CYBER

File Name
Addressing Human Factors Gaps in Cyber Defense
Cyber Gray Space Deterrence
Cyber Security Workforce Development and the Protection of Critical Infrastructure
Discovering Neighbor Devices in Computer Network
Framework for Designing Realistic Cyber Warfare Exercises
Intelligent Software Decoy Tools for Cyber
Making Sense of Email Addresses on Drives
MIL-STD-1553B protocol covert channel analysis
Modeling Cyber-Physical War-Gaming
Network-Enabled Operations - Social Network Analysis of Information Sharing
NEXT GENERATION REPOSITORY FOR SHARING SENSITIVE NETWORK AND SECURITY DATA
Russia's Approach to Cyber Warfare
Trusted Computer Exemplar -Physical Security Plan
Trusted Computing Exemplar -Configuration Management Procedures

DECLASSIFIED

File Name
11 September 2001 - With the President
Alleged New Type of Soviet Submarine
Application of Cluster Analysis - the Voynich Manuscript
CIA Accountability Before and After 9-11
CIA Sculpture Study Group
Conversion of Soviet Naval Vesels to Nuclear Propulsion and Rocket Weapons
Effectiveness of the CIA Counterterrorist Interrogation Techniques
Estimated Partial Afterburning Performance J-58 Engine
German Radio Intelligence
Inspection Report of the DCI Counterterrorist Center
John Nash Letters

POLICY

File Name
Analysis of government policies to support sustainable domestic defense industries
Breaking monetary policy rules in Russia
China's Economic Statecraft in Latin America
China's evolving foreign policy in Africa
Government Policy with Time Inconsistent Voters
Implications of Potential Chinese Missile Defense for U.S. Security Interests
Offense-defense theory analysis of Russian cyber capability
Patenting and Innovation in China
Review of China policy of OED sea use
Russia’s Monetary Policy
Russia's natural gas policy toward Northeast Asia
Vietnam’s drive to modernize military - causes and implications

SCIENCE AND TECHNOLOGY

File Name
A Robust Event-Triggered Approach for Fast Sampled-Data Extremization and Learning
Breakthrough technologies - Robotics, Innovation, and Intellectual Property
Experimental and theoretical investigations of quantum state transfer and decoherence
Hybrid Multiobjective Optimization Algorithm for PM Motor Design
Joint Machine Learning and Game Theory for Rate Control in High Efficiency Video Coding
Linearization of Bipolar Amplifiers Based on Neural-Network Training Algorithm
Multi-Task Convolutional Neural Network for Pose-Invariant Face Recognition
Opportunistic Refreshing Algorithm for eDRAM Memories
Parallel distinguishability of quantum operations
Quantum-secured blockchain
Semisupervised Incremental Support Vector Machine Learning Based on Neighborhood Kernel Estimation
The Chopthin Algorithm for Resampling
Uncertainty Quantification in Mathematics-Embedded Ontologies Using Stochastic Reduced Order Model

SPACE

File Name
Addressing and Presenting Quality of Satellite Data via Web-based Services
Cryogenic fiber optic assemblies for spaceflight environments
Entry, Descent, and Landing Performance for a Mid-Lift-to-Drag Ratio Vehicle at Mars
Exploring the Limits of High Altitude GPS for Future Lunar Missions
Nuclear Cryogenic Propulsion Stage (NCPS) Fuel Element Testing in the Nuclear Thermal Rocket Element Environmental Simulator (NTREES)
Optimization of a Lunar Pallet Lander Reinforcement Structure using a Genetic Algorithm
Program to Optimize Simulated Trajectories II Surrogate Models for Mars Ascent Vehicle Performance Assessment
Propulsion Trade Studies for Spacecraft Swarm Mission Design
Safe Haven Configurations for Deep Space Transit Habitats
Space Shuttle Program Dual Docked Operations
Summary of the NASA Design Environment for Novel Vertical Lift Vehicles (DELIVER) Project
Use of Shuttle Heritage Hardware in Space Launch System Application-Structural Assessment

SPECIAL OPERATIONS

File Name
Analysis of Special Operation Command's Management of Weapon System Programs
Enhancing SOF through UAV Pinpoint Payload Delivery
Global SOF Network- Posturing Special Operations Forces to Ensure Global Security
Life Cycle Management for the Special Operations Craft Riverine
MICROHEMATURIA ASSOCIATED WITH A SPECIAL OPERATIONS
Multimodal Displays in Army Human-Robot Operations
Navy Irregular Warfare and Counterterrorism Operations
Roles of Perseverance, Cognitive Ability, and Pysical Fitness - U.S. Army Special Forces
Sensing Capability for Naval Special Warfare METOC Support
Special Operations Forces and CIA Paramilitary Operations -Issues for Congress

SUBSURFACE

File Name
Utilizing Ocean Thermal Energy in a Submarine Robot
US Navy Submarine Sea Trial of NASA developed Multi-Gas Monitor
Three-Dimensional Path Palnning Method for Autonomous Underwater Vehicle Based on Modified Firefly Algorithm
Phase I Final Report- Titan Submarine
Optimization of Antennas of the EISS Radar Designed to Perform Deep Martian Subsurface Sounding
Navy Trident Submarine Conversion (SSGN) Program
Navy Attack Submarine Force-Level - Goal and Procurement Rate
Magnetic Subsurface Imaging Systems in a Smartphone Based on the Built-In Magetometer
Improved OTEC System for a Submarine Robot
Improved Discrimination of Subsurface Targets Using a Polarization-Sensitive Directional Borehole Radar
Feasibility and Conceptual Design Study for Towed Torpedo Emulator
Airborne Internet Access Through Submarine Optical Fiber Cables

SURFACE

File Name
A HYBRID AGENT APPROACH FOR SET-BASED CONCEPTUAL SHIP DESIGN
A Salvo Model of Warships in Missile Combat Used to Evaluate Staying Power
An inverse hull design approach in minimizing the ship wave
DDG-1000 missile integration
Establishing the Fundamentals of a Surface Ship Survivability Design Discipline
Hydrodynamic optimization of ship hull forms
Hydrostatic and hydrodynamic analysis of a lengthened DDG-51
Navy DDG-51 and DDG-1000 Destroyer Programs - Background and Issues
NURBS_skinning_surface_for_ship_hull_design_based_
Plastic sheer buckling of ship hull plating induced by grounding
Quasi-developable B-spline surfaces in ship hull design
Sonar signal acquisition and processing for identification and classification of ship hull fouling

WEAPONS SYSTEMS

File Name
Aluminum Micro-Balloons as Improved Fuel for Warhead Explosives
Applied Explosives Technology
Attribution and Forensic Science in Addressing Biological Weapon Threats
Bioeffects on an In Vitro Model by Small-Scale Explosives and Shock Wave Overpressure Impacts
Energetic Materials for Bio-Agent Destruction
Enhanced Performance From Insensitive Explosives
European Trilateral Nuclear Dialogues
Hybrid Rocket Experiment Station for Capstone Design
Nuclear Explosives - Technology for On-site Inspection
On Lethal Autonomous Weapons
Ultrafast laser spectroscopy of shock wave dynamics in explosive materials

APPENDIX B. HONEYPOT WEBSITE SITEMAP

```
<?xml version="1.0" encoding="UTF-8"?>
<urlset
      xmlns="http://www.sitemaps.org/schemas/sitemap/0.9"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.sitemaps.org/schemas/
sitemap/0.9
            http://www.sitemaps.org/schemas/sitemap/0.9/
sitemap.xsd">
<!-- created with Free Online Sitemap Generator www.xml-
sitemaps.com -->


<url>
  <loc>http://www.nps-future-research.org/</loc>
  <lastmod>2018-05-04T22:08:09+00:00</lastmod>
  <priority>1.00</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/air.html</loc>
  <lastmod>2018-05-03T19:20:11+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/budget.html</loc>
  <lastmod>2018-05-03T19:20:48+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/cyber.html</loc>
  <lastmod>2018-05-03T19:21:27+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/declassified.html</loc>
  <lastmod>2018-05-03T19:22:08+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/policy.html</loc>
  <lastmod>2018-05-03T19:22:54+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/science-tech.html</loc>
  <lastmod>2018-05-03T19:23:32+00:00</lastmod>
  <priority>0.80</priority>
</url>
```

```
<url>
  <loc>http://www.nps-future-research.org/space.html</loc>
  <lastmod>2018-05-03T19:24:17+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/spec-ops.html</loc>
  <lastmod>2018-05-03T19:24:57+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/subsurface.html</loc>
  <lastmod>2018-05-03T19:25:32+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/surface.html</loc>
  <lastmod>2018-05-03T19:26:08+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/weapons.html</loc>
  <lastmod>2018-05-03T19:41:35+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/index.html</loc>
  <lastmod>2018-05-04T22:08:09+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Air/
Advanced%20Aerobots%20for%20Scientific%20Exploration.pdf</loc>
  <lastmod>2018-04-17T01:35:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Air/
Artificial%20Intelligence%20Based%20Control%20Power%20Optimizatio
n%20on%20Tailless%20Aircraft.pdf</loc>
  <lastmod>2018-04-17T01:35:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Air/
Command%20and%20control%20models%20of%20next%20generation%20unman
ned%20aircraft%20systems.pdf</loc>
  <lastmod>2018-04-17T01:35:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
```

```
<url>
  <loc>http://www.nps-future-research.org/Air/
Design%20Process%20of%20Flight%20Vehicle%20Structures%20for%20a%2
0Common%20Bulkhead%20and%20an%20MPCV%20Spacecraft%20Adapter.pdf</
loc>
  <lastmod>2018-04-17T01:35:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Air/F-
35%20Alternate%20Engine%20Program.pdf</loc>
  <lastmod>2018-04-17T01:35:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Air/F-
35%20Aluminum%20Composite%20Stack%20Drilling.pdf</loc>
  <lastmod>2018-04-17T01:35:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Air/
Flight%20Vehicle%20Structural%20Design%20Processes%20for%20a%20Co
mmon%20Bulkhead%20and%20a%20Multipurpose%20Crew%20Vehicle%20Space
craft%20Adapter.pdf</loc>
  <lastmod>2018-04-17T01:35:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Air/
High%20energy%20solid%20state%20and%20free%20electron%20laser%20s
ystems%20in%20tactical%20aviation.pdf</loc>
  <lastmod>2018-04-17T01:35:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Air/
Investigation%20of%20Missile%20Control%20Surface%20Effects%20on%2
0F-16%20Limit-Cycle%20Oscillation.pdf</loc>
  <lastmod>2018-04-17T01:35:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Air/
Subsonic%20Ultra%20Green%20Aircraft%20Research%20-
%20Hybrid%20Electric%20Design%20Exploration.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
```

```
  <loc>http://www.nps-future-research.org/Air/
UAV%20Supervisory%20Control%20on%20F-
18%20Formation%20Flight%20Performance.pdf</loc>
  <lastmod>2018-04-17T01:36:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
America%20First%20-
%20A%20Budget%20Blueprint%20to%20Make%20America%20Great%20Again.p
df</loc>
  <lastmod>2018-04-17T01:36:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
An%20Update%20to%20the%20Budget%20and%20Economic%20Outlook%20-
%202017%20to%202027.pdf</loc>
  <lastmod>2018-04-17T01:37:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
Cash%20and%20Accrual%20Measures%20in%20Federal%20Budgeting.pdf</l
oc>
  <lastmod>2018-04-17T01:37:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/Counter-
ISIS%20Train%20and%20Equip%20Fund.pdf</loc>
  <lastmod>2018-04-17T01:37:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
DARPA%20Funds%20Surprising%20Systems.pdf</loc>
  <lastmod>2018-04-17T01:37:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
Federal%20Debt%20and%20the%20Statutory%20Limit,%20January%202018.
pdf</loc>
  <lastmod>2018-04-17T01:37:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
```

```
  <loc>http://www.nps-future-research.org/Budget/
Inflation%20and%20Price%20Escalation%20Adustments%20-%20F-
35.pdf</loc>
  <lastmod>2018-04-17T01:37:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/Long-
Range%20Plan%20for%20Construction%20of%20Naval%20Vessels%20for%20
Fiscal%20Year%202019.pdf</loc>
  <lastmod>2018-04-17T01:37:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
Military%20Personnel%20Programs.pdf</loc>
  <lastmod>2018-04-17T01:37:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
Options%20for%20Reducing%20the%20Deficit%20-
%202017%20to%202026.pdf</loc>
  <lastmod>2018-04-17T01:37:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
Program%20Acquisition%20Cost%20by%20Weapon%20System.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
Research%20Development,%20Test%20&amp;%20Evaluation%20Programs.pd
f</loc>
  <lastmod>2018-04-17T01:38:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/
The%20Acceptability%20of%20War%20and%20Support%20for%20Defense%20
Spending.pdf</loc>
  <lastmod>2018-04-17T01:38:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Budget/The%20Depot-
Level%20Maintenance%20of%20DoD's%20Combat%20Aircraft%20-
%20Insights%20for%20the%20F-35.pdf</loc>
```

```
  <lastmod>2018-04-17T01:38:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
Addressing%20Human%20Factors%20Gaps%20in%20Cyber%20Defense.pdf</l
oc>
  <lastmod>2018-04-17T01:38:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
Cyber%20Gray%20Space%20Deterrence.pdf</loc>
  <lastmod>2018-04-17T01:38:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
Cyber%20Security%20Workforce%20Development%20and%20the%20Protecti
on%20of%20Critical%20Infrastructure.pdf</loc>
  <lastmod>2018-04-17T01:38:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
Discovering%20Neighbor%20Devices%20in%20Computer%20Network.pdf</l
oc>
  <lastmod>2018-04-17T01:39:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
Framework%20for%20Designing%20Realistic%20Cyber%20Warfare%20Exerc
ises.pdf</loc>
  <lastmod>2018-04-17T01:39:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
Intelligent%20Software%20Decoy%20Tools%20for%20Cyber.pdf</loc>
  <lastmod>2018-04-17T01:39:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/MIL-STD-
1553B%20protocol%20covert%20channel%20analysis.pdf</loc>
  <lastmod>2018-04-17T01:39:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
```

```
  <loc>http://www.nps-future-research.org/Cyber/
Making%20Sense%20of%20Email%20Addresses%20on%20Drives.pdf</loc>
  <lastmod>2018-04-17T01:39:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/Modeling%20Cyber-
Physical%20War-Gaming.pdf</loc>
  <lastmod>2018-04-17T01:39:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
NEXT%20GENERATION%20REPOSITORY%20FOR%20SHARING%20SENSITIVE%20NETW
ORK%20AND%20SECURITY%20DATA.pdf</loc>
  <lastmod>2018-04-17T01:40:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/Network-
Enabled%20Operations%20-
%20Social%20Network%20Analysis%20of%20Information%20Sharing.pdf</
loc>
  <lastmod>2018-04-17T01:39:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
Russia%D1%82%D0%90%D0%A9s%20Approach%20to%20Cyber%20Warfare.pdf</
loc>
  <lastmod>2018-04-17T01:40:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
Trusted%20Computer%20Exemplar%20-
Physical%20Security%20Plan.pdf</loc>
  <lastmod>2018-04-17T01:40:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Cyber/
Trusted%20Computing%20Exemplar%20-
Configuration%20Management%20Procedures.pdf</loc>
  <lastmod>2018-04-17T01:40:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
```

```
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/11%20September%202001%20-
%20With%20the%20President.pdf</loc>
  <lastmod>2018-04-17T01:40:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/
Alleged%20New%20Type%20of%20Soviet%20Submarine.pdf</loc>
  <lastmod>2018-04-17T01:40:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/Application%20of%20Cluster%20Analysis%20-
%20the%20Voynich%20Manuscript.pdf</loc>
  <lastmod>2018-04-17T01:40:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/
CIA%20Accountability%20Before%20and%20After%209-11.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/CIA%20Sculpture%20Study%20Group.pdf</loc>
  <lastmod>2018-04-17T01:42:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/
Conversion%20of%20Soviet%20Naval%20Vesels%20to%20Nuclear%20Propul
sion%20and%20Rocket%20Weapons.pdf</loc>
  <lastmod>2018-04-17T01:42:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/
Effectiveness%20of%20the%20CIA%20Counterterrorist%20Interrogation
%20Techniques.pdf</loc>
  <lastmod>2018-04-17T01:42:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
```

```
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/
Estimated%20Partial%20Afterburning%20Performance%20J-
58%20Engine.pdf</loc>
  <lastmod>2018-04-17T01:42:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/German%20Radio%20Intelligence.pdf</loc>
  <lastmod>2018-04-17T01:42:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/
Inspection%20Report%20of%20the%20DCI%20Counterterrorist%20Center.
pdf</loc>
  <lastmod>2018-04-17T01:42:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Declassified%20Projects/John%20Nash%20Letters.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
Analysis%20of%20government%20policies%20to%20support%20sustainabl
e%20domestic%20defense%20industries.pdf</loc>
  <lastmod>2018-04-17T01:42:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
Breaking%20monetary%20policy%20rules%20in%20Russia.pdf</loc>
  <lastmod>2018-04-17T01:42:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
China's%20Economic%20Statecraft%20in%20Latin%20America.pdf</loc>
  <lastmod>2018-04-17T01:42:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
China's%20evolving%20foreign%20policy%20in%20Africa.pdf</loc>
  <lastmod>2018-04-17T01:43:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
Government%20Policy%20with%20Time%20Inconsistent%20Voters.pdf</lo
c>
  <lastmod>2018-04-17T01:43:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
Implications%20of%20Potential%20Chinese%20Missile%20Defense%20for
%20U.S.%20Security%20Interests.pdf</loc>
  <lastmod>2018-04-17T01:43:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/Offense-
defense%20theory%20analysis%20of%20Russian%20cyber%20capability.p
df</loc>
  <lastmod>2018-04-17T01:43:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
Patenting%20and%20Innovation%20in%20China.pdf</loc>
  <lastmod>2018-04-17T01:43:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
Review%20of%20China%20policy%20of%20OED%20sea%20use.pdf</loc>
  <lastmod>2018-04-17T01:43:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
Russia's%20natural%20gas%20policy%20toward%20Northeast%20Asia.pdf
</loc>
  <lastmod>2018-04-17T01:43:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Policy/
Russia%D1%82%D0%90%D0%A9s%20Monetary%20Policy.pdf</loc>
  <lastmod>2018-04-17T01:43:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
```

```
  <loc>http://www.nps-future-research.org/Policy/
Vietnam%D1%82%D0%90%D0%A9s%20drive%20to%20modernize%20military%20
-%20causes%20and%20implications.pdf</loc>
  <lastmod>2018-04-17T01:44:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/A%20Robust%20Event-
Triggered%20Approach%20for%20Fast%20Sampled-
Data%20Extremization%20and%20Learning.pdf</loc>
  <lastmod>2018-04-17T01:44:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/Breakthrough%20technologies%20-
%20Robotics,%20Innovation,%20and%20Intellectual%20Property.pdf</l
oc>
  <lastmod>2018-04-17T01:44:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/
Experimental%20and%20theoretical%20investigations%20of%20quantum%
20state%20transfer%20and%20decoherence.pdf</loc>
  <lastmod>2018-04-17T01:44:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/
Hybrid%20Multiobjective%20Optimization%20Algorithm%20for%20PM%20M
otor%20Design.pdf</loc>
  <lastmod>2018-04-17T01:44:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/
Joint%20Machine%20Learning%20and%20Game%20Theory%20for%20Rate%20C
ontrol%20in%20High%20Efficiency%20Video%20Coding.pdf</loc>
  <lastmod>2018-04-17T01:44:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/
```

```
Linearization%20of%20Bipolar%20Amplifiers%20Based%20on%20Neural-
Network%20Training%20Algorithm.pdf</loc>
  <lastmod>2018-04-17T01:44:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/Multi-
Task%20Convolutional%20Neural%20Network%20for%20Pose-
Invariant%20Face%20Recognition.pdf</loc>
  <lastmod>2018-04-17T01:45:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/
Opportunistic%20Refreshing%20Algorithm%20for%20eDRAM%20Memories.p
df</loc>
  <lastmod>2018-04-17T01:45:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/
Parallel%20distinguishability%20of%20quantum%20operations.pdf</lo
c>
  <lastmod>2018-04-17T01:45:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/Quantum-
secured%20blockchain.pdf</loc>
  <lastmod>2018-04-17T01:46:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/
Semisupervised%20Incremental%20Support%20Vector%20Machine%20Learn
ing%20Based%20on%20Neighborhood%20Kernel%20Estimation.pdf</loc>
  <lastmod>2018-04-17T01:46:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/
The%20Chopthin%20Algorithm%20for%20Resampling.pdf</loc>
  <lastmod>2018-04-17T01:46:00+00:00</lastmod>
  <priority>0.64</priority>
```

```
</url>
<url>
  <loc>http://www.nps-future-research.org/
Science%20&amp;%20Technology/
Uncertainty%20Quantification%20in%20Mathematics-
Embedded%20Ontologies%20Using%20Stochastic%20Reduced%20Order%20Mo
del.pdf</loc>
  <lastmod>2018-04-17T01:46:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Addressing%20and%20Presenting%20Quality%20of%20Satellite%20Data%2
0via%20Web-based%20Services.pdf</loc>
  <lastmod>2018-04-17T01:46:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Cryogenic%20fiber%20optic%20assemblies%20for%20spaceflight%20envi
ronments.pdf</loc>
  <lastmod>2018-04-17T01:46:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Entry,%20Descent,%20and%20Landing%20Performance%20for%20a%20Mid-
Lift-to-Drag%20Ratio%20Vehicle%20at%20Mars.pdf</loc>
  <lastmod>2018-04-17T01:47:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Exploring%20the%20Limits%20of%20High%20Altitude%20GPS%20for%20Fut
ure%20Lunar%20Missions.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Nuclear%20Cryogenic%20Propulsion%20Stage%20(NCPS)%20Fuel%20Elemen
t%20Testing%20in%20the%20Nuclear%20Thermal%20Rocket%20Element%20E
nvironmental%20Simulator%20(NTREES).pdf</loc>
  <lastmod>2018-04-17T01:47:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Optimization%20of%20a%20Lunar%20Pallet%20Lander%20Reinforcement%2
0Structure%20using%20a%20Genetic%20Algorithm.pdf</loc>
```

```
  <lastmod>2018-04-17T01:47:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Program%20to%20Optimize%20Simulated%20Trajectories%20II%20Surroga
te%20Models%20for%20Mars%20Ascent%20Vehicle%20Performance%20Asses
sment.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Propulsion%20Trade%20Studies%20for%20Spacecraft%20Swarm%20Mission
%20Design.pdf</loc>
  <lastmod>2018-04-17T01:48:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Safe%20Haven%20Configurations%20for%20Deep%20Space%20Transit%20Ha
bitats.pdf</loc>
  <lastmod>2018-04-17T01:49:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Space%20Shuttle%20Program%20Dual%20Docked%20Operations.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Summary%20of%20the%20NASA%20Design%20Environment%20for%20Novel%20
Vertical%20Lift%20Vehicles%20(DELIVER)%20Project.pdf</loc>
  <lastmod>2018-04-17T01:49:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Space/
Use%20of%20Shuttle%20Heritage%20Hardware%20in%20Space%20Launch%20
System%20Application-Structural%20Assessment.pdf</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
Analysis%20of%20Special%20Operation%20Command's%20Management%20of
%20Weapon%20System%20Programs.pdf</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
Enhancing%20SOF%20through%20UAV%20Pinpoint%20Payload%20Delivery.p
df</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
Global%20SOF%20Network-
%20Posturing%20Special%20Operations%20Forces%20to%20Ensure%20Glob
al%20Security.pdf</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
Life%20Cycle%20Management%20for%20the%20Special%20Operations%20Cr
aft%20Riverine.pdf</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
MICROHEMATURIA%20ASSOCIATED%20WITH%20A%20SPECIAL%20OPERATIONS.pdf
</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
Multimodal%20Displays%20in%20Army%20Human-
Robot%20Operations.pdf</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
Navy%20Irregular%20Warfare%20and%20Counterterrorism%20Operations.
pdf</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
Roles%20of%20Perseverance,%20Cognitive%20Ability,%20and%20Pysical
%20Fitness%20-%20U.S.%20Army%20Special%20Forces.pdf</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
Sensing%20Capability%20for%20Naval%20Special%20Warfare%20METOC%20
Support.pdf</loc>
  <lastmod>2018-04-17T01:50:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Special%20Operations/
Special%20Operations%20Forces%20and%20CIA%20Paramilitary%20Operat
ions%20-Issues%20for%20Congress.pdf</loc>
  <lastmod>2018-04-17T01:51:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Airborne%20Internet%20Access%20Through%20Submarine%20Optical%20Fi
ber%20Cables.pdf</loc>
  <lastmod>2018-04-17T01:51:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Feasibility%20and%20Conceptual%20Design%20Study%20for%20Towed%20T
orpedo%20Emulator.pdf</loc>
  <lastmod>2018-04-17T01:51:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Improved%20Discrimination%20of%20Subsurface%20Targets%20Using%20a
%20Polarization-
Sensitive%20Directional%20Borehole%20Radar.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Improved%20OTEC%20System%20for%20a%20Submarine%20Robot.pdf</loc>
  <lastmod>2018-04-17T01:52:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Magnetic%20Subsurface%20Imaging%20Systems%20in%20a%20Smartphone%2
0Based%20on%20the%20Built-In%20Magetometer.pdf</loc>
  <lastmod>2018-04-17T01:52:00+00:00</lastmod>
  <priority>0.64</priority>
```

```
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Navy%20Attack%20Submarine%20Force-Level%20-
%20Goal%20and%20Procurement%20Rate.pdf</loc>
  <lastmod>2018-04-17T01:52:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Navy%20Trident%20Submarine%20Conversion%20(SSGN)%20Program.pdf</l
oc>
  <lastmod>2018-04-17T01:52:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Optimization%20of%20Antennas%20of%20the%20EISS%20Radar%20Designed
%20to%20Perform%20Deep%20Martian%20Subsurface%20Sounding.pdf</loc
>
  <lastmod>2018-04-17T01:52:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Phase%20I%20Final%20Report-%20Titan%20Submarine.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/Three-
Dimensional%20Path%20Palnning%20Method%20for%20Autonomous%20Under
water%20Vehicle%20Based%20on%20Modified%20Firefly%20Algorithm.pdf
</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
US%20Navy%20Submarine%20Sea%20Trial%20of%20NASA%20developed%20Mul
ti-Gas%20Monitor.pdf</loc>
  <lastmod>2018-04-17T01:54:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Subsurface/
Utilizing%20Ocean%20Thermal%20Energy%20in%20a%20Submarine%20Robot
.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
```

```
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/
A%20HYBRID%20AGENT%20APPROACH%20FOR%20SET-
BASED%20CONCEPTUAL%20SHIP%20DESIGN.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/
A%20Salvo%20Model%20of%20Warships%20in%20Missile%20Combat%20Used%
20to%20Evaluate%20Staying%20Power.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/
An%20inverse%20hull%20design%20approach%20in%20minimizing%20the%2
0ship%20wave.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/DDG-
1000%20missile%20integration.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/
Establishing%20the%20Fundamentals%20of%20a%20SurJace%20Ship%20Sur
vivability%20Design%20Discipline.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/
Hydrodynamic%20optimization%20of%20ship%20hull%20forms.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/
Hydrostatic%20and%20hydrodynamic%20analysis%20of%20a%20lengthened
%20DDG-51.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
```

```
  <loc>http://www.nps-future-research.org/Surface/
NURBS_skinning_surface_for_ship_hull_design_based_.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/Navy%20DDG-
51%20and%20DDG-1000%20Destroyer%20Programs%20-
%20Background%20and%20Issues.pdf</loc>
  <lastmod>2018-04-17T01:55:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/
Plastic%20sheer%20buckling%20of%20ship%20hull%20plating%20induced
%20by%20grounding.pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/Quasi-
developable%20B-
spline%20surfaces%20in%20ship%20hull%20design.pdf</loc>
  <lastmod>2018-04-17T01:57:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Surface/
Sonar%20signal%20acquisition%20and%20processing%20for%20identific
ation%20and%20classification%20of%20ship%20hull%20fouling.pdf</lo
c>
  <lastmod>2018-04-17T01:57:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
Aluminum%20Micro-
Balloons%20as%20Improved%20Fuel%20for%20Warhead%20Explosives.pdf<
/loc>
  <lastmod>2018-04-17T01:57:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
Applied%20Explosives%20Technology.pdf</loc>
  <lastmod>2018-04-17T01:57:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
```

```
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
Attribution%20and%20Forensic%20Science%20in%20Addressing%20Biolog
ical%20Weapon%20Threats.pdf</loc>
  <lastmod>2018-04-17T01:57:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
Bioeffects%20on%20an%20In%20Vitro%20Model%20by%20Small-
Scale%20Explosives%20and%20Shock%20Wave%20Overpressure%20Impacts.
pdf</loc>
  <lastmod>2018-04-17T01:57:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
Energetic%20Materials%20for%20Bio-
Agent%20%20Destruction.pdf</loc>
  <lastmod>2018-04-17T01:58:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
Enhanced%20Performance%20From%20Insensitive%20Explosives.pdf</loc
>
  <lastmod>2018-04-17T01:58:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
European%20Trilateral%20Nuclear%20Dialogues.pdf</loc>
  <lastmod>2018-04-17T01:58:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
Hybrid%20Rocket%20Experiment%20Station%20for%20Capstone%20Design.
pdf</loc>
  <lastmod>2018-05-07T00:42:43+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
Nuclear%20Explosives%20-%20Technology%20for%20On-
site%20Inspection.pdf</loc>
  <lastmod>2018-04-17T02:01:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
```

```
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
On%20Lethal%20Autonomous%20Weapons.pdf</loc>
  <lastmod>2018-04-17T02:01:00+00:00</lastmod>
  <priority>0.64</priority>
</url>
<url>
  <loc>http://www.nps-future-research.org/Weapons%20Systems/
Ultrafast%20laser%20spectroscopy%20of%20shock%20wave%20dynamics%2
0in%20explosive%20materials.pdf</loc>
  <lastmod>2018-04-17T02:01:00+00:00</lastmod>
  <priority>0.64</priority>
</url>


</urlset>
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. SURVEY QUESTIONNAIRE

A Honeypot for Spies Survey

Would you assume that the Naval Postgraduate School (NPS) owns and maintains this website?

What details or characteristics make you think that the site is or is not a legitimate NPS resource?

If you were unsure of the website's legitimacy, is it compelling enough for you to continue exploring and browsing the webpage and subpages?

Which categories seem most interesting or most important?

If you were tasked with collecting information on the United States Department of Defense and you found this website, in which category would you focus your collection efforts?

Are there any specific documents that appear particularly compelling?

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Altwaijry, H., & Shahbar, K. (2013). (WHASG) Automatic SNORT signatures generation by using honeypot. *Journal of Computers*, *8*(12), 3280-3286. https://doi.org/10.4304/jcp.8.12.3280-3286

Anuar, N.B., Zakaria, O., & Chong, W.Y. (2006). Honeypot through Web (Honeyd@WEB): The emerging of security application integration. *Issues in Informing Science & Information Technology*, *f*(45), 45–56. https://doi.org/ 10.28945/871

Apache. (2012, November 29). Httpd Wiki ProxyAbuse. Retrieved from https://wiki.apache.org/httpd/ProxyAbuse

Bacon, D.J. (1998). *Second World War deception: Lessons learned for today's joint planner* (Wright Flyer Paper No. 5). Maxwell Air Force Base, AL: Air Command and Staff College, Air University.

Bodmer, S., Kilger, M., Carpenter, G., Jones, J., & Jones, J. (2012). Cyber Counterintelligence. In *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. New York, NY: McGraw-Hill. http://techbus.safaribooks online.com/book/networking/security/9780071772495/chapter-3-cyber-counterintelligence/c24.

Cheswick, B. (1992). An evening with Berferd in which a cracker is lured, endured, and studied. *Proceedings of the Winter USENIX Conference*, 163–174. Retrieved from http://www.cheswick.com/ches/papers/berferd.pdf

Coyle, G.A., & Wilson, A. (2014). Haversack ruses—From leather to digital. *International Journal of Intelligence and CounterIntelligence, 27*(1): 156–177. https://doi.org/10.1080/08850607.2013.807197

Department of Defense. (2011). *Department of Defense strategy for operating in cyberspace*. Retrieved from https://csrc.nist.gov/CSRC/media/Projects/ISPAB/ documents/DoD-Strategy-for-Operating-in-Cyberspace.pdf

Department of Defense. (2015). *The Department of Defense cyber strategy*. Retrieved from https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/ Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

Destailleur, L. (n.d.). AWStats documentation - Glossary. Retrieved October 17, 2018, from https://awstats.sourceforge.io/docs/awstats_glossary.html

Djanali, S., Arunanto, F., Pratomo, B.A., Baihaqi, A., Studiawan, H., & Shiddiqi, A.M. (2014). Aggressive web application honeypot for exposing attacker's identity. *Proceedings of the 1st International Conference on Information Technology, Computer, and Electrical Engineering*, 212–216. https://doi.org.10.1109/ ICITACEE.2014.7065744

Gartzke, E. & Lindsay, J.R. (2015) Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348. https://doi.org/ 10.1080/09636412.2015.1038188

Google Analytics. (2018). The difference between Google ADs clicks, and sessions, users, entrances, pageviews, and unique pageviews in Analytics - Analytics Help. Retrieved from https://support.google.com/analytics/answer/1257084?hl=en

Johnson, W.R. (2009). *Thwarting enemies at home and abroad: How to be a counterintelligence officer*. Washington, DC: Georgetown University Press. https://ebookcentral.proquest.com/lib/ebook-nps/detail.action?docID=449336

Joshi, R. C., & Sardana, A. (2011). *Honeypots: a new paradigm to information security*. Boca Raton, FL: CRC Press. Retrieved from https://www-taylorfrancis-com.libproxy.nps.edu/books/9781439869994

Lynn, W. (2010). Defending a new domain. *Foreign Affairs*, *89*(5), 97–108. Retrieved from http://search.proquest.com/docview/749414296/.

Nicomette, V., Kaaniche, M., Alata, E., & Herrb, M. (2011). Set-up and deployment of a high-interaction honeypot: Experiment and lessons learned. *Journal in Computer Virology*, *7*(2), 143–157. https://doi.org/10.1007/s11416-010-0144-2

Office of the Director of National Intelligence. (2011). *U.S. national intelligence, an overview*. Washington, DC: Government Publishing Office. Retrieved from https://permanent.access.gpo.gov/gpo19700/ICConsumersGuide2011.pdf

Provos, N. (2004). A virtual honeypot framework. *Proceedings of the 13th USENIX Security Symposium,* 1–14. Retrieved from http://static.usenix.org/event/sec04/ tech/full_papers/provos/provos_html/

Rafalko, F. (2004). *Counterintelligence reader American Revolution to World War II.* Washington, DC: National Counterintelligence Center. Retrieved from https://permanent.access.gpo.gov/lps54742/counterintelligencereader/ci/docs/ci1/ ch1a.htm

Rodriguez-Hernandez, S.M. (2013). Counterintelligence. In *Encyclopedia of Military Science,* 412–414. Retrieved from http://sk.sagepub.com/reference/encyclopedia-of-military-science/i4886.xml

Rowe, N. (2006). Measuring the effectiveness of honeypot counter-counterdeception. In system sciences. *Proceedings of the 39th Annual Hawaii International Conference, 6*, 129c–129c. https://doi.org/10.1109/HICSS.2006.269

Rowe, N.C. (2018). *Honeypot deception tactics*. Draft.

Rowe, N.C., & Rrushi, J. (2016). *Introduction to cyberdeception*. https://doi.org/10.1007/978-3-319-41187-3

Schmitt, M (2013). Rule 61 – Ruses. In *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York, NY: Cambridge University Press. Retrieved from http://techbus.safaribooksonline.com/book/current-affairs/9781107301535/glossary/glossary_html

Singer, P., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. New York, NY: Oxford University Press.

Spitzner, L. (2002). *Honeypots: Tracking hackers.* Retrieved from https://techbus.safaribooksonline.com/0-321-10895-7

Stoll, C. (1990). *The cuckoo's egg: Tracking a spy through the maze of computer espionage*. New York, NY: Pocket Books.

Studiawan, H., Djanali, S., & Pratomo, B. (2016). Graph-based forensic analysis of web honeypot. *Journal of Telecommunications and Information Technology* (2), 60–65. Retrieved from https://www.researchgate.net/publication/305374359_Graph-based_forensic_analysis_of_web_honeypot

Sun Tzu (1971). *The art of war*. London, UK: Oxford University Press.

UltimateWB. (2014, February 10). Google Analytics vs Awstats – Which is better, more accurate, useful? Retrieved from https://www.ultimatewb.com/blog/674/google-analytics-vs-awstats-which-is-better-more-accurate-useful/

Weiss, G.W. (2007). *The farewell dossier: Duping the Soviets*. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm

Whitham, B. (2013). Automating the generation of fake documents to detect network intruders. *International Journal of Cyber-Security and Digital Forensics*, *2*(1), 103-118. Retrieved from http://sdiwc.net/digital-library/automating-the-generation-of-fake-documents-to-detect-networkintruders

Yagi, T., Tanimoto, N., Hariu, T., & Itoh, M. (2010). Enhanced attack collection scheme on high-interaction web honeypots. *Proceedings of the IEEE Symposium on Computers and Communications*, 81–86. https://doi.org/10.1109/ISCC.2010.554670

Zhuang, J., Bier, V., & Alagoz, O. (2010). Modeling secrecy and deception in a multiple-period attacker–defender signaling game. *European Journal of Operational Research*, *203*(2), 409–418. https://doi.org/doi:10.1016/j.ejor.2009.07.028

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California