PsychNology Journal, 2011
Volume 9, Number 2, 79-122

Scientometrics of Deception, Counter-deception, and Deception Detection in Cyber-space

Frank Stech[1], Kristin E. Heckman[1*], Phil Hilliard[1] and Janice R. Ballo[1]

[1]The MITRE Corporation
(USA)

ABSTRACT

The concepts of deception, counter-deception, and deception detection in the cyber-space domain have been the subject of little systematic analysis. Our objective was to conduct scientometric analyses of these concepts in the cyber-space domain. We observed the following: Although various deceptive tactics are addressed in the cyber-security literature, it appears they are characterized more from the standpoint of technology than from their social, behavioral, or cognitive elements; these cyber-tactics are not mapped into the classic components of denial and deception tactics; there is no conventional terminology to describe the phenomenon of deception in cyber-space; classic deception domain terminology is rarely used; and classic deception domain researchers are rarely cited. These observations suggest that cyber-deception is an emerging field.

Keywords: *scientometrics, cyber-deception, cyber-counter-deception, cyber-deception detection, deception, cyber-space*

Paper Received 27/04/2011; received in revised form 15/09/2011; accepted 30/11/2011.

1. Introduction

Deception has been defined in the literature in a number of ways. It has been defined in general terms (e.g., Masip, et al., 2004; National Research Council, 1991), and in attempts to develop a psychology of deception (Hyman, 1989). It has also been defined in conjunction with frameworks for scientific theories of deception (e.g., Buller & Burgoon, 1994; Daniel & Herbig, 1982; Deception Research Program, 1979; Ekman, 1985; Epstein, 1989; Heuer, 1981; Heuer, 1982; Whaley, 1982) and in conjunction with frameworks of deception based on folk psychology (e.g., Coleman & Kay, 1981;

Cite as:
Stech, F., & Heckman, K. (2011). Scientometrics of Deception, Counter-deception, and Deception Detection in Cyber-space. *PsychNology Journal, 9*(2), 79 – 122. Retrieved [month] [day], [year], from www.psychnology.org.

*Corresponding Author:
Kristin E. Heckman
The MITRE Corporation, M/S N720, 7515 Colshire Drive, McLean, VA 22102,
E-mail: kheckman@mitre.org

Ekman & Friesen, 1969; Goffman, 1959; Goffman, 1974; Hopper & Bell, 1984; Saarni, 1982). We refer to deception as any false belief held by an individual or group of individuals as a result of sensory information acquired via verbal or non-verbal means, or as a result of sensory information misperceptions. Based on this definition, deception can occur without a "deceiver," and thus can also occur without intent. For example, amputees can be deceived into believing they still have their amputated limb because of the "phantom" pain or sensations they experience (Ramachandran & Rogers-Ramachandran, 1996).

Deception in the physical world is a ubiquitous phenomenon. Intuitively, it would seem that the same would be true in the virtual world. Cyber-deception runs the gamut from deceptive online advertising to individuals falsifying their personal characteristics in online dating services; from cyber-espionage to lying in email or via a VoIP conversation; and from cyber-crime to news outlets "Photoshopping" online news article images. We therefore refer to cyber-deception as deception resulting from the transmission of information via the Internet. Although we recognize that cyber-space consists of a broad set of literature that includes sub-fields such as cyber-deception, cyber-security, cyber-law, and cyber-psychology among others, for the purposes of this paper, we refer to cyber-space as the set of literature including cyber-security, computer science, and information security given our intent to better understand how computer scientists and engineers address cyber-deception. We envision the field of cyber-space literature as a Venn diagram with many intersections among all these sub-fields.

There has been little systematic analysis of the concepts of deception, counter-deception, and deception detection in the cyber-space domain (Yuill, Denning, and Feer, 2006). Much more comprehensive analysis exists in the domain of classic deception research. This is problematic given the many types of cyber-deception, including offensive and defensive deception, and the probability that many more remain unexplored. Similarly, deception, counter-deception, and deception detection can be automated in cyber-space. Both offensive and defensive tactics are necessary in any cyber-war arena. More knowledge is needed to detect, employ, and counter deception in cyber-space to enhance the security of computers and networks. The resulting knowledge can then be translated into security practices.

Our objective was to conduct scientometric analyses of deception, counter-deception, and deception detection in the cyber-space domain, both to characterize the research that has been done, and to determine promising directions for discoveries and innovations in future research. Scientometrics is a process to measure and analyze science that can help identify trends, patterns, relationships, and associations.

We conducted comprehensive literature searches in two scholarly databases (Engineering Village and Web of Science) to identify cyber-deception literature in the subject areas of cyber-security, computer science, and information security and to create a database of the citation records. We then analyzed the citation record data using scientometric clustering and full-text extraction tools.

Our results show that there is not a discrete, clearly identifiable body of cyber-deception literature. This may be the result of cyber-deception researchers not using deception domain terminology, which, in turn, may be the result of cyber-deception researchers infrequently citing classic deception domain researchers. This suggests that cyber-deception is an emerging field with a relatively immature body of literature. Despite this, there does appear to be a small set of topical areas, including computer mediated communication and deception detection, in which cyber-deception research is active.

Our analyses also revealed several themes associated with the clusters of literature which had the highest number of articles related to deception. These themes include psychology, decision making, communication/linguistics, virtual reality, and computer games.

Although deceptive tactics such as phishing, spamming, hacking, computer espionage, and honey pots and nets are described in the cyber-space literature from a technical perspective, there is little analysis of the social, behavioral, or cognitive elements of these tactics. Nor are these cyber-tactics mapped into the components of denial and deception tactics as described in the classic deception domain literature. Finally, unlike the classic deception research literature, there are no general frameworks in the cyber-space literature of theories or tactics of cyber-deception.

We suggest that future work should include further analysis of the literature we identified as being most related to deception, to identify the subset of literature that truly constitutes cyber-deception. A full set of scientometric analyses can then be conducted on these cyber-deception articles to learn the keyword terms used in cyber-deception research, key concepts and themes, research approaches, and key researchers and centers of research. In turn, these details from the core literature of cyber-deception research can then be mapped to the corresponding categories in the literature of classic deception research to thus identify gaps, overlaps, commonalities, and differences.

We also suggest that future work should include building a terminology bridge between the cyber-space and the deception domains. This effort could result in a process to identify and map the tools, techniques, and practices used by researchers, planners, and practitioners in these two domains.

Identifying the research gaps by analyzing the cyber-deception literature and developing a framework with a terminology bridge, will provide the foundation to facilitate addressing the research gaps through the development of offensive and defensive cyber-deception tools, techniques, and practices that are grounded in the latest, most advanced science. Such mappings identify opportunities for fruitful cross-disciplinary deception and counter-deception research, and thereby help develop new knowledge in the cyber-deception and counter-deception domains.

2. Method

Scientometrics refers to the process of measuring and analyzing science. Scientometrics can help identify trends, patterns, relationships, and associations. Scientometrics is useful in determining in a particular science what areas are being developed, where they are being developed, and who is developing them. The typical scientometrics indicator is based on measurements of scientific communications, such as bibliometrics about scientific publications (journals, patents); administrative communications concerning science and technology (patents, grants, financials); or some other observable and scientific relationship that can be analyzed and counted (Glänzel, 2010).

The availability of large online databases of scientific publications and sophisticated tools for measuring, correlating, and analyzing a variety of dimensions of scientific publications allow for both broad and detailed characterization surveys of the research landscape, including retrospective, inferential, deductive, and abductive analyses. Scientometric characterization studies determine (among other things): top researchers and research institutions; patterns and trends across countries (including anomalies); taxonomies or clusters of research themes and key concepts; trends in research across time, themes, institutions and researchers; research networks and affiliations among researchers, institutions, themes; and indicators of research publication.

The literature search and scientometrics processes are tightly coupled and iterative in that the results of initial scientometric analysis are used to refine the search strategy to provide a more relevant set of data on which to perform the analysis.

For this project we conducted broad and focused literature searches in Engineering Village (EV) and Web of Science (WoS) databases. These databases comprehensively index journals and conference proceedings in cyber-security and related subject areas of computer science and information security. Citation retrievals were downloaded to EndNote X3, a bibliographic management program. Because there is overlap between the content indexed by these two databases, Endnote proved effective for identifying and removing duplicate citations before conducting the scientometric analysis.

The initial literature search used broad concepts to retrieve as many records as possible related to cyber-security and deception. Terminology in the cyber domain is evolving and many concepts are expressed in various forms (e.g., cybersecurity and cyber-security). Consequently, in the initial broad search statements "cyber" was truncated in order to catch all the variations. Deception, counter-deception, deception detection terms were then linked with "cyber," and related terms such as "online," "internet," "information security." Cyber-security related terms were also searched in the titles of articles to capture literature in which the concept of deception in cyber-space may be addressed but not specifically stated as such. The first phase of literature searches was analyzed using the scientometrics tools and then more focused searches were conducted using key terms identified in the clustering process: social engineering, phishing, steganography, encryption, honeypots, propaganda, spam, virtual reality, viruses, and malware. Figure 1 shows the concepts used in literature keyword searches throughout the iterative literature search process.

We imported all record results from keyword searches into a scientometrics tool called VantagePoint (version 6.0)[1] and then clustered the records into groups with similar themes using a term clustering tool called CLUTO (version 1.1)[2]. Clustering is a process within scientometrics that gathers closely related articles into groups based on similar key characteristics such as keywords, abstract phrases, or title phrases. The clustering process is useful to determine articles that are similar, authors that may be working on the same topic, or institutions that may be prominent in a particular area of research.

[1] http://www.thevantagepoint.com/
[2] http://glaros.dtc.umn.edu/gkhome/views/cluto

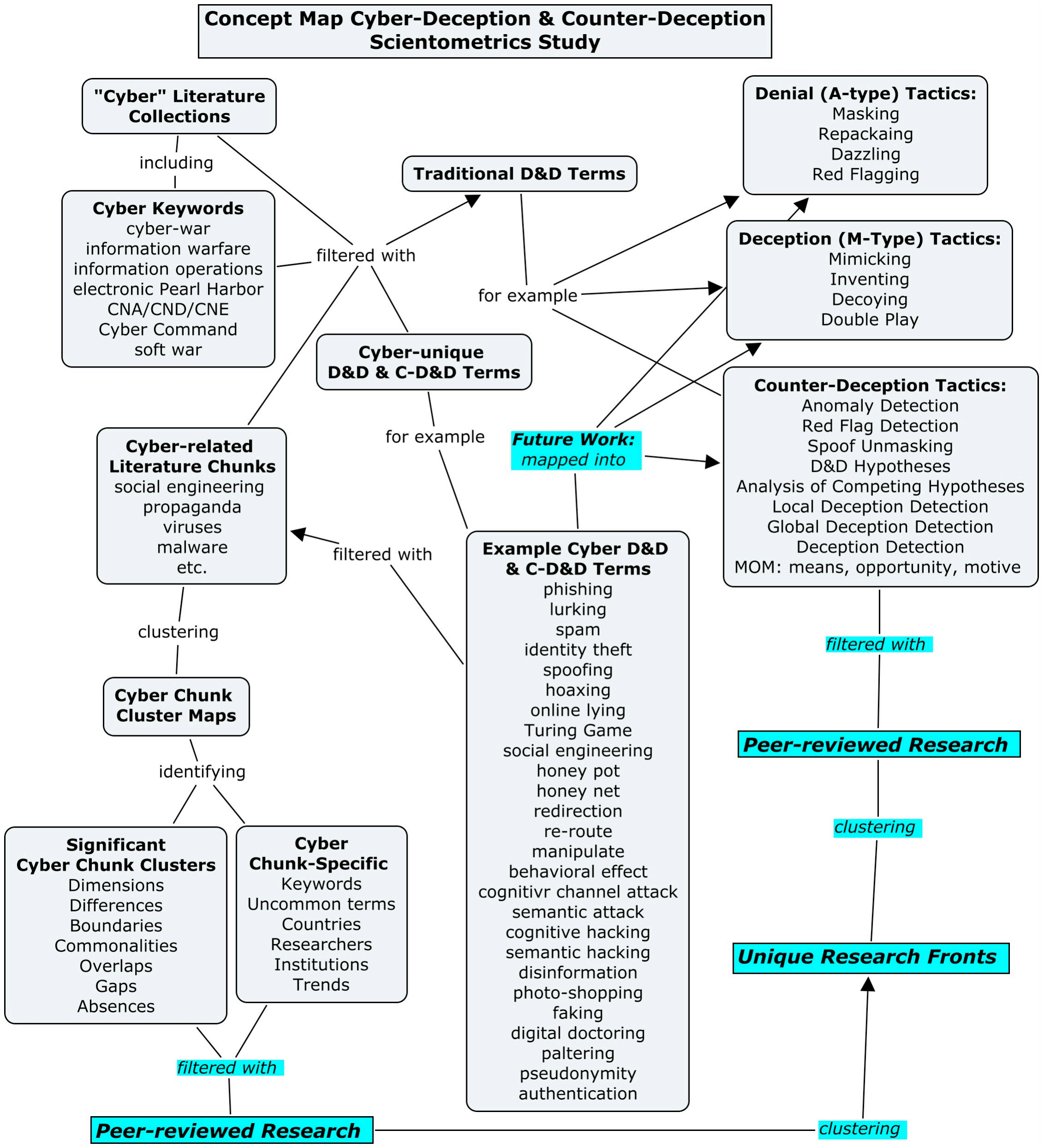

Figure 1. Deception and Cyber-deception Search Terms. Concept map depicts the iterative relationships between processes used to identify relevant cyber, and traditional denial and deception (D&D) and counter-denial and deception (C-D&D), keywords, and apply these to select papers to develop literature-based cyber concept “literature chunks” and clusters for filtering the collected cyber literature. This filtering then produced literature –based cluster maps, and inputs to the scientometric analysis tools to identify significant cyber chunk clusters (e.g., dimensions) and chunk-specific keywords (e.g., uncommon terms, countries, researchers). Areas in blue indicate processes for seeding future scientometric studies by comparing and contrasting cyber-deception and traditional deception research literatures to identify promising unique research fronts.

After clustering the records, they were examined for key characteristics such as top keywords, abstract phrases, journal titles, and institutions. These characteristics were then used to form a “theme” around each cluster. The analyst assigned these themes by manually examining the characteristics of each cluster. Next, the analyst developed relevant observations and recommendations. The analysts' observations after conducting the focused literature search led us to conduct an additional analysis to investigate the use of deception terminology by cyber-deception researchers. This was a two-pronged analysis conducted in Excel and a full-text extraction tool called ExtPhr32 (version 1.2.6.6)[3] using a set of cyber-deception literature identified by a subject matter expert (SME). The Excel analysis measured the frequency of deception terms and concepts in a subset of the SME-identified cyber-deception literature. It also measured the frequency of citations to deception domain literature from this subset of SME-identified literature.

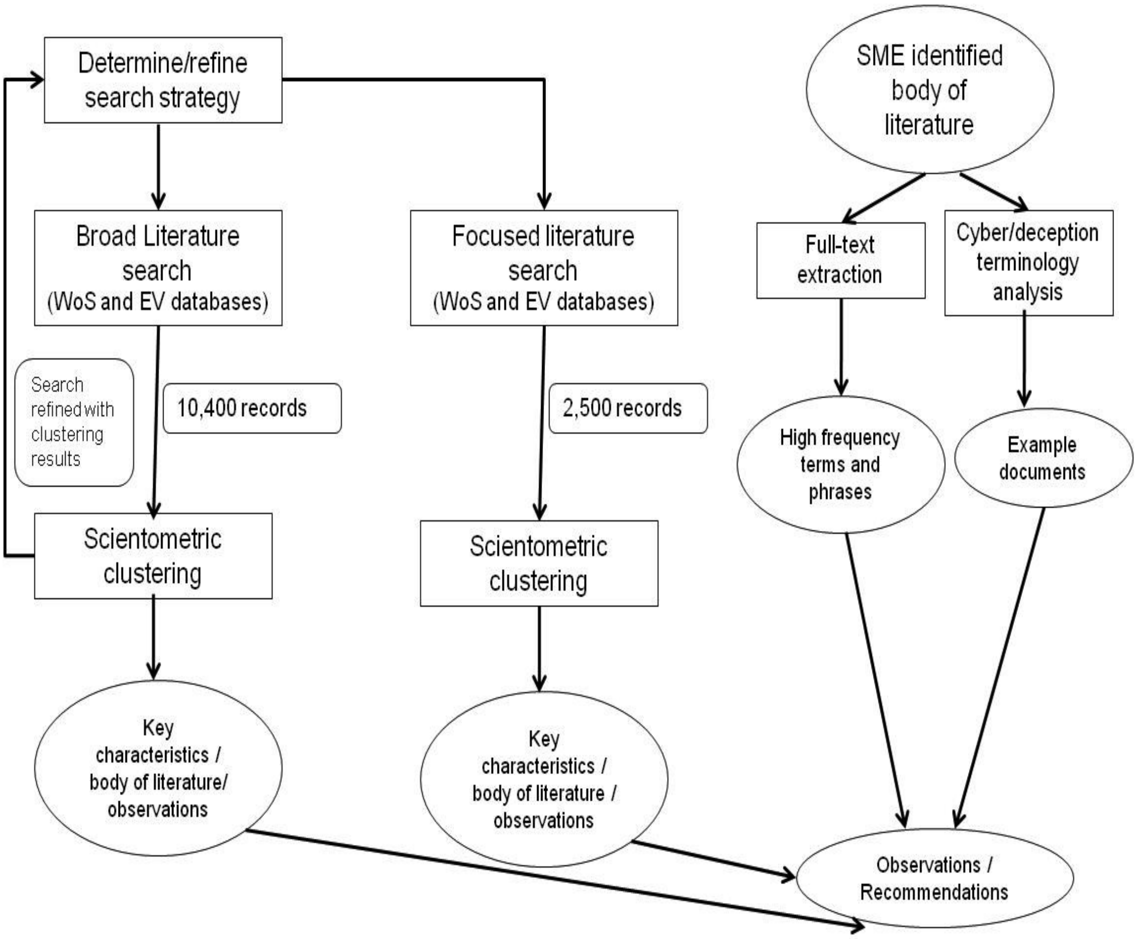
Determine/refine search strategy
Broad Literature search (WoS and EV databases)
Focused literature search (WoS and EV databases)
SME identified body of literature
Full-text extraction
Cyber/deception terminology analysis
Search refined with clustering results
10,400 records
2,500 records
High frequency terms and phrases
Example documents
Scientometric clustering
Scientometric clustering
Key characteristics / body of literature/ observations
Key characteristics / body of literature / observations
Observations / Recommendations

Figure 2. Solution Method Process Diagram.

[3] http://publish.uwo.ca/~craven/freeware.htm

The ExtPhr32 analysis used full-text extraction. Full-text extraction is a technique that can identify high-frequency terms and phrases that may not be tagged as a “keyword” for the article or may not be listed in the abstract for the article. Hence, full-text extraction can identify somewhat oblique themes that may not be readily apparent within a set of documents. Figure 2 illustrates these steps via a process diagram.

3. Results

3.1 Scientometric Analyses

The initial broad literature search yielded almost 14,000 citation records, which were analyzed using scientometric clustering tools. We examined the resulting clusters and noted that there were groups, comprising over 1,200 records, related to “cybernetics” that were not particularly relevant to our topic. In our next iteration of the literature search, records with “cybernetics” were eliminated from the resulting data set.

Our refined data set from the broad literature search contained approximately 10,500 records. These records were clustered and examined for key characteristics such as top keywords, abstract phrases, journal titles, and institutions. The analyst then used these characteristics to form a “theme” around each cluster. These clusters and themes are shown in Table 1.

Two clusters, Cluster 7 and Cluster 19, were identified as having key characteristics that were closely related to deception. Cluster 7 (231 records) contains articles closely related to deception, decision making, problem solving, and agents. Cluster 19 (252 records) contains articles related to psychology, deception, and deception detection. The key characteristics and articles in these clusters are listed in Appendix A.

Examining these “deception-related” clusters yields some information regarding what areas in cyber-deception are indeed being researched. The psychology of deception and deception detection emerge as two possible themes that researchers are studying.

One notable key characteristic in these two clusters is the authors that are represented. In cluster 19, the authors Judee Burgoon and Jay Nunamaker are represented with 34 and 28 articles, respectively. Based on their deception domain knowledge, the principal investigators identify Burgoon and Nunamaker as two prominent authors in classical deception literature.

Cluster	*# Records*	*Possible Theme*
30	883	Computer crime
31	664	Information security, systems analysis
27	562	Hackers, viruses, malware
25	506	Law, regulation, privacy
29	486	Networks
26	458	Electronic commerce, business
28	457	Human factors, social aspects of computing
18	453	Education
22	394	Data security, information security, management
24	386	Network security, cryptography
12	385	Intrusion detection
20	335	Process control, control systems
14	326	Cyber-space (miscellaneous – legal, security, virtual reality)
9	318	Health, telemedicine
23	314	Virtual reality, human factors, user interfaces
21	312	Risk management, risk assessment, risk analysis
16	308	Cryptography
11	306	Telecommunication security, honeypots, intrusion detection
15	283	Watermarking
19	252	Deception, psychology, deception detection
8	232	Data protection, privacy
7	231	Decision making, problem solving, deception, agents
1	200	RADAR jamming, deception jamming
10	192	Algorithms, problem solving, deception
13	192	Artificial intelligence, robots
6	169	Cryptography, authentication,
17	166	Seismology, earthquakes (cluster resulting from ‘Deception Island’)
2	160	Computer programming, computer software
5	158	Cyber-security, chemical industry
4	134	Computer crime, legislation,
3	120	Embedded systems, cyber-physical systems
0	88	Undetermined
-1	7	Undetermined

Table 1. Broad Literature Search Cluster Themes.

These authors often focus their research in the areas of computer-mediated communication and deception detection. This seems to indicate that these are areas that are being investigated.

The focused literature search used terms closely related to cyber and deception such as “social engineering.” These terms were searched separately in the databases. Table 2 indicates the search term used and the number of records retrieved from these searches.

Key Search Term	*# Records*
Encryption	805
Honeypots	65
Propaganda	98
Social engineering	258
Spam	112
Steganography	602
Virtual reality	519
Viruses malware	272

Table 2. Focused Literature Search Terms and Resulting Records.

Cluster Number	*# Records*	*Possible Themes*
30	156	Virtual reality, human computer interaction, computer simulation
29	123	Cryptography, stegnanography
21	119	Cryptography, stegnanography
15	118	Intrusion detection, networks
16	112	Social engineering, data security
31	108	Virtual reality, marketing, artificial intelligence
12	104	Cryptography, encryption, decryption
8	102	Cryptography, chaotic systems
6	97	Cryptography, images, holography
26	94	Virtual reality, computer simulation
28	90	Cryptography, security of data, authentication
25	81	Cryptography, computer graphics,
4	72	Cryptography, embedded systems, advanced encryption standards
23	70	Computer viruses, malware
22	69	Virtual reality, augmented reality, sensors
7	68	Watermarking, digital watermarking
1	65	Fourier transforms, computer simulation
11	62	Computer networks, computer viruses
3	59	Phishing, social engineering
19	58	Robotics, computer simulation
27	55	Computer crime, computer security, data privacy
14	53	Virtual reality, education, computer aided instruction
17	52	Data security (conference proceedings)
20	51	Social engineering, authentication
10	49	Public key cryptography, data security
13	48	Chemistry, biology
9	46	Linguistics, language, text processing
18	39	Cryptography, Data privacy,
24	39	Computer simulation, biological viruses
5	36	E-mail, spam
2	35	Imaging, models
0	31	Honeypots, computer networks

Table 3. Focused Literature Search Cluster Themes.

Approximately 2,400 total records resulted from these searches. These records were combined into one data set for scientometric analysis and clustering. As in the broad literature search, we examined these clusters to determine their theme and possible relevance to deception and fraud. Table 3 shows the number of records in each cluster and possible themes derived from the key characteristics of each cluster.

As we expected, clusters tended to form around the focused search terms because the clustering algorithm uses keywords as one of its variables to form clusters. In this analysis, a “deception” theme was not readily apparent in the more targeted search clusters. However, themes did form around terms closely related to deception such as cryptography, social engineering, and phishing.

This cluster formation led us to hypothesize that while the articles may be related to deception, their key characteristics, such as keywords, abstract phrases, and titles, may not indicate so. This may mean that authors and database indexes are not using deception-related terms to classify their articles. There are two different sets of nomenclature that are not intersecting: one related to cyber-space and one related to deception. To further investigate this hypothesis, we examined a set of literature known to be related to cyber-deception research to determine whether deception domain terminology is used by cyber-deception researchers (See Section 3.2 Deception Terminology Analysis). We also examined this set of literature with full-text extraction (See Section 3.3 Full-Text Extraction) to identify high-frequency terms and phrases.

3.2 Deception Terminology Analysis

We conducted an analysis to test our hypothesis that cyber-deception researchers do not use the same terminology as deception domain researchers. To do this we used a set of literature containing approximately 50 items that had already been vetted by a SME as representative of cyber-deception research (See Appendix C SME-Identified Cyber-Deception Literature). This set of documents was independent from the resulting documents in the literature searches previously described. From this set of SME-identified literature we selected a subset for our analysis which included published scholarly papers, conference proceedings, and unpublished manuscripts. We excluded government documents, theses, dissertations, books, book reviews, briefing slides, popular press articles, and workshop reports. The final set included 22 papers.

The first step in the analysis was to select deception-specific terminology based on reading the abstract and introduction, and skimming the remainder of the paper. These terms were compiled into a list, and a running tally was kept for the number of occurrences of each term across all 22 papers. Table 4 shows the list of deception terms/concepts, the number of occurrences in the 22 papers, and the frequency ratio.

Term/Concept	*Total Uses of Term/Concept*	*Frequency Ratio*
deception	18	82%
denial (of service or information)	11	50%
manipulate	9	41%
truth/trustworthiness	8	36%
misinformation	6	27%
influence (perceptions & behavior)	6	27%
falsification (of indicators or ID)	6	27%
concealing	4	18%
mislead	4	18%
perception management	4	18%
social engineering	3	14%
lie	3	14%
countermeasures	2	9%
distortion	2	9%
decoy	2	9%
feint	2	9%
ruse	2	9%
espionage	2	9%
stealth	2	9%
dazzle	2	9%
decoy	2	9%
hoax	2	9%
spoofing	1	5%
propaganda	1	5%
counter-deception	1	5%
display	1	5%
demonstration	1	5%
covert action	1	5%
psyops	1	5%
counterfeit	1	5%
cover	1	5%
misrepresentation	1	5%
dissimulation	1	5%
simulation	1	5%
masking	1	5%
repackaging	1	5%
inventing	1	5%
mimicking	1	5%

Table 4. Deception Terms/Concepts Used in Cyber-deception Papers.

Note that the term "deception" was the most frequently used, that is, it was used in 82% of the papers. This is worth noting, because all 22 papers were clearly about some aspect of deception, yet the term was not used in all 22 papers.

The analysis showed that the authors used from 2 to 13 deception terms/concepts in each paper. Figure 3 shows the correspondence between the 22 papers analyzed and the number of deception terms/concepts occurrences. Almost half of the papers (i.e., 9) used 3 or 4 deception terms/concepts. Only one paper used the maximum number of deception terms/concepts (i.e., 13).

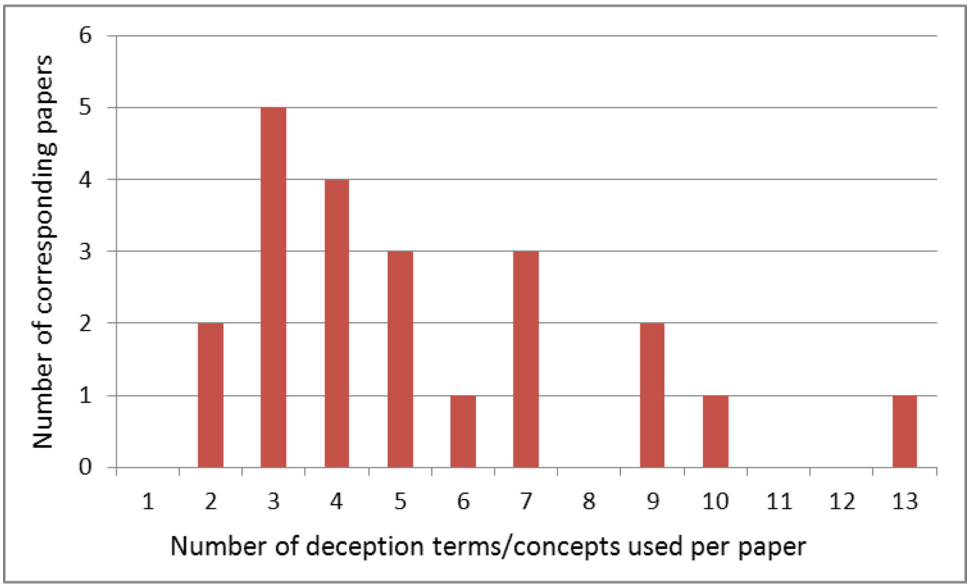

Figure 3. Use of Deception Terms/Concepts in Cyber deception Papers.

Our tentative conclusion from this analysis was that cyber-deception researchers do use deception terminology, but not as frequently as might be expected. As an example, one paper postulated a new term, cognitive hacking, as follows: "Provision of misinformation, the intentional distribution or insertion of false or misleading information intended to influence reader's decisions and/or activities, is a form of cognitive hacking" (Thompson, 2004). Deception domain researchers would refer to this as propaganda.

This led us to hypothesize that cyber-deception researchers rarely cite deception domain literature. To test this hypothesis we again analyzed the same set of 22 papers. We began by assembling a list of the most proficient/impactful deception domain authors whose area(s) of specialty included deception in: general, communication theory, military, and intelligence.

Author	Total Citations	Frequency Ratio
Bell, J. Bowyer	1	5%
Birchmeier, Zachary	1	5%
Buller, David	3	14%
Burgoon, Judee	4	18%
Camden, Carl	1	5%
Carlson, John	2	9%
Caspi, Avner	1	5%
Cialdini, Robert	1	5%
von Clausewitz, Claude	1	5%
DePaulo, Bella	1	5%
DePaulo, Peter	0	0%
Donath, Judith	1	5%
Ekman, Paul	2	9%
Frank, Mark	0	0%
George, Joey	1	5%
Goffman, Erving	2	9%
Golder, Scott	1	5%
Grazioli, Stefano	1	5%
Hale, Jerold	1	5%
Hancock, Jeffrey	2	9%
Handel, Michael	0	0%
Haselton, Martie	1	5%
Heuer, Richards	1	5%
Hollingshead, Andrea	1	5%
Huff, Darrell	1	5%
Jervis, Robert	0	0%
Jones, Gerald	1	5%
Jones, Reginald	0	0%
Kalbfleisch, Peter	1	5%
Knapp, Mark	1	5%
Kraut, Robert	1	5%
Lewicki, Roy	1	5%
Masip, Jaume	1	5%
Nunamaker, Jay	0	0%
Pratkanis, Anthony	1	5%
Tsu, Sun	1	5%
Twitchell, Douglas	0	0%
Utz, Sonja	1	5%
Vrij, Aldert	1	5%
Whaley, Barton	1	5%
Zhou, Lina	3	14%
Zuckerman, Miron	1	5%

Table 5. Deception Authors Cited by Cyber-deception Researchers.

We then reviewed the references section of each paper, and added to this list any additional cited authors of deception papers, and kept a running tally of the number of papers which cited these authors (See Table 5). We then computed a frequency ratio for each author. Judee Burgoon was the most frequently cited author, although her work was only cited by 4 of the 22 papers analyzed. Burgoon's research areas of specialty include deception in general and deception in communication theory. Note that authors in Table 5 with 0 citations are authors we initially selected given their proficiency and/or the impact of their work in the selected topic areas; however, they were not cited by any of the papers analyzed.

Figure 4 shows the number of deception author citations per paper. The number of citations ranged from 0 to 15. Half of the papers analyzed (i.e., 11) did not cite a single deception researcher. Only one paper cited 15 deception researchers.

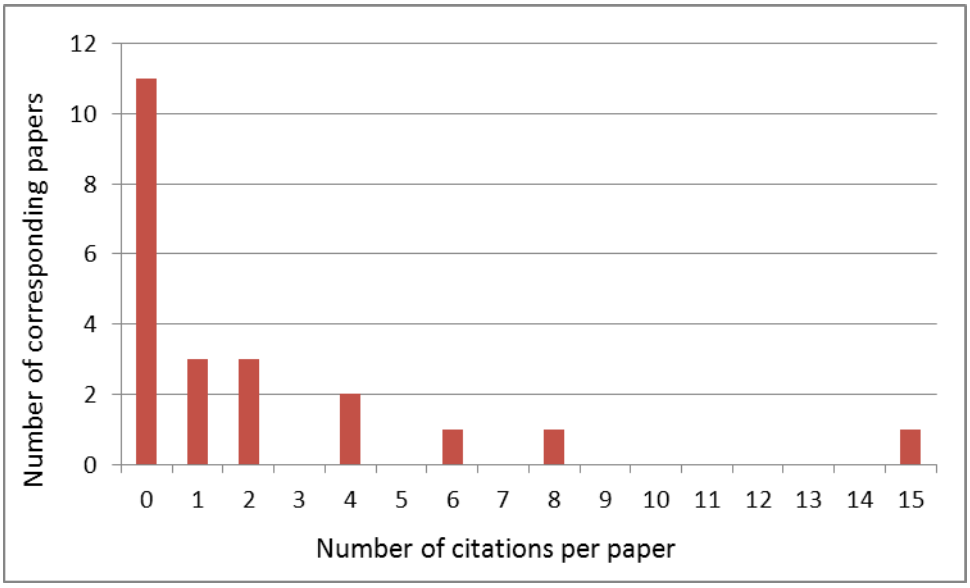

Figure 4. Use of Citations to Deception Authors

These results, combined with those from the first analysis, led us to conclude that cyber-deception researchers, in general, do not cite the deception domain literature, and consequently do not use deception domain terminology.

3.3 Full-Text Extraction

To identify any other high-frequency words and phrases that may be associated in the cyber-deception domain, we performed a full-text extraction analysis on the entire set of 50 SME-identified papers. These documents were analyzed using a full-text extraction tool called ExtrPhr32, to extract the most high-frequency terms and phrases. ExtrPhr32 takes a text-file as input and can identify how often terms and multi-word phrases appear in the file.

Results from the full-text extraction indicated that high-frequency terms and phrases are closely related to national security and military operations. For example, the most common terms in this set of documents were: UNITED STATES, CYBER-WARFARE, AIR FORCE, NATIONAL SECURITY and INFORMATION WARFARE. A more complete list is included in Appendix B.

4. Discussion

There appears to be little cross-disciplinary literature pertaining to cyber-deception in the science and technology focused databases we examined. Two research elements support this observation: (a) the focused literature search that contained search terms relevant to cyber-deception did not reveal a significant body of literature that identified itself (through keywords or abstract-phrases) as being related to deception; and (b) examination of SME-identified cyber-deception literature suggested that deception domain terminology is loosely and infrequently used by cyber-deception researchers. Our analysis suggested that the latter may be due to the fact that cyber-deception researchers do not frequently cite classic deception domain researchers.

In addition, an earlier scientometric analysis by one of the authors (Lorber & Stech, 2009) surveyed a broad range of scientific and technical (S&T) publications (20,085 articles) related to truth-telling and deception phenomena. These articles were obtained through queries regarding information gathering, information communication, deception, deception detection, and related themes in five databases: Thomson Reuters Science Citation Index, Social Science Citation Index,[4] Medline,[5] PsycINFO[6] and Engineering Village.[7] Three clusters of articles were found related to the social,

[4] The Thomson Reuters Science Citation Index (SCI) and Social Science Citation Index (SSCI) include approximately 6,500 journals covering a wide range of scientific disciplines. Records consist of bibliographic data (typically including abstracts), institution data for all co-authors, not just the lead author, and cited records, offering a powerful pathway to link ideas, people, and institutions.

[5] Medline is a life sciences-focused citation database maintained by NIH. Medline indexes roughly 5,500 journals that routinely dedicate coverage to the life sciences. It is considered to be the premier English language data source for research in the life sciences.

[6] PsycINFO is a database of research abstracts provided by the American Psychological Association with systematic coverage of the psychological literature from the 1800s to the present. (The database also includes records from the 1600s and 1700s.) PsycINFO contains bibliographic citations, abstracts, cited references, and descriptive information.

[7] Elsevier's EngineeringVillage comprises Compendex and Inspec, two discrete databases which partially overlap, share the EngineeringVillage search interface, and can be concurrently or independently searched. Compendex covers over 5,600 journals and conference

behavioral, and medical sciences research on deception and deception detection: (a) Deception-Law Enforcement (fraud and abuse, white collar crime, guilt and deception detection, and polygraphy); (b) Deception-Personality Psychology (deception, lying, and truth-telling, such as verbal and non-verbal behaviors, and cultural or developmental aspects of truth-telling and lying; lying behaviors of children; ethics and morality related to lying); and (c) Deception Detection (deception, communication, behavior, cues, deception detection, lies, accuracy, lie detection, interpersonal deception).

Tables 6, 7, and 8 show the authors, journals, and keywords of the social, behavioral, and medical sciences research surveyed by Lorber & Stech (2009) on deception and deception detection. These authors, journals, and keywords have only some overlap (shown in italics) in authors, none in journals, and very little overlap in keywords when compared to the largely technical literature on cyber-deception (see Tables 4 and 5 above, and Tables in Appendix A).

Authors	Journals	Keywords
Gershon Ben Shakhar (38)	Journal of Applied Psychology (57)	*deception* (87)
Eitan Elaad (37)	Psychophysiology (43)	polygraph (60)
Charles R. Honts (21)	International Journal of Psychophysiology (26)	fraud (47)
Peter J. Rosenfeld (18)	Journal of Police Science and Administration (14)	lie detection (42)
M.T. Bradley (17)	Journal of Forensic Sciences (13)	guilty knowledge test (34)
H.N. Pontell (15)	Crime Law and Social Change (13)	psychophysiological detection (29)
Bruno Verschuere (13)	Perceptual and Motor Skills (11)	validity (27)
William Iacono (13)	Physiology & Behavior (10)	crime (26)
John J. Furedy (11)	Law and Human Behavior (10)	accuracy (26)
Geert Crombez (11)	Kriminalistik (10)	information (22)

Table 6. Top Ten Authors, Journals, and Keywords (and frequencies) in the Deception-Law Enforcement Cluster (from Lorber & Stech, 2009). Overlap with the cyber-deception technical literature shown in italics.

proceedings (~11.3 million records) primarily from the fields of chemical, civil, electrical, mechanical, and mining engineering. Inspec focuses more heavily on physics, computing, information technology, and network and security topics, but also covers some engineering domains covered by Compendex. Inspec indexes roughly 11 million records.

Authors	Journals	Keywords
Aldert Vrij (80)	Law and Human Behavior (36)	*deception* (163)
Bella Depaulo (40)	Journal of Personality and Social Psychology (33)	lying (79)
Victoria Talwar (21)	Applied Cognitive Psychology (27)	*lies* (65)
Paul Ekman (20)	Child Development (19)	lie detection (54)
Kerry Lee (19)	Journal of Nonverbal Behavior (18)	*truth* (53)
Ray Bull (19)	Personality and Social Psychology Bulletin (17)	behavior (40)
Kang Lee (17)	Personality and Individual Differences (15)	deceit (31)
Par Anders Granhag (17)	Legal and Criminological Psychology (13)	deception detection (28)
M.G. Frank (15)	Communication Monographs (13)	cues (27)
Lucy Akehurst (15)	Psychological Reports (12)	ability (27)

Table 7. Top Ten Authors, Journals, and Keywords (and frequencies) in the Deception-Personality Psychology Cluster (from Lorber & Stech, 2009). Overlap with the cyber-deception technical literature shown in italics.

Authors	Journals	Keywords
Judee Burgoon (68)	Journal of Nonverbal Behavior (48)	*deception* (297)
Bella Depaulo (33)	Journal of Personality and Social Psychology (40)	deception detection (62)
Jay Nunamaker (28)	Personality and Social Psychology Bulletin (30)	communication (44)
David Buller (28)	Human Communication Research (26)	behavior (39)
Miron Zuckerman (23)	Communication Monographs (22)	cues (37)
Aldert Vrij (23)	American Psychologist (19)	interpersonal deception (32)
Joey George (22)	Law and Human Behavior (18)	deception[8] (32)
Par Anders Granhag (2)	Group Decision and Negotiation (18)	accuracy (29)
Martin Orne (16)	Ethics & Behavior (17)	information (22)
Robert Feldman (15)	Perceptual and Motor Skills (16)	*lies* (20)

Table 8. Top Ten Authors, Journals, and Keywords (and frequencies) in the Deception Detection Cluster (from Lorber & Stech, 2009). Overlap with the cyber-deception technical literature shown in italics.

Authors that have a relatively large number of papers in our cyber data set (such as Judee Burgoon and Jay Nunamaker) are researching computer mediated communication and deception detection. This suggests that there is ongoing research around these areas related to cyber-space and deception. Other themes in our analysis of the cyber literature surrounding the clusters with the highest number of articles related to deception are psychology, decision making, communication/linguistics, virtual reality, and computer games. Further literature research focusing specifically on these topic areas is needed to discover how much of that literature is related to the cyber domain.

Although deceptive tactics such as phishing, spamming, hacking, computer espionage, and honey pots are described in the cyber-security literature, it appears the research is characterized more from the standpoint of technology; with little analysis of the social, behavioral, or cognitive elements of these tactics. Nor are these cyber-

[8] Deception was any hyphenated term ending in "deception," such as "self-deception."

tactics mapped into the components of denial and deception tactics as described in the classic deception literature surveyed by Lorber and Stech (2009). Finally, unlike the classic deception research literature, there are no general frameworks in the cyber literature of theories or tactics of cyber-deception.

The full-text extraction analysis of the sampled cyber research papers indicated that the set of SME-identified cyber-deception literature is closely related to military operations or national security. It may be beneficial to examine other databases such as Dissertation Abstracts International or Defense Technical Information Center (DTIC) to capture more of this research.

Based on these results, it appears that cyber-deception is an emerging field with a relatively immature body of research. Because of this, its literature is not discrete, and therefore not easily identifiable. We propose that there would be more synergy in cyber-deception research if cyber-space, deception domain, and cyber-deception researchers were reading and using each other's work, a theme echoed in a recent volume advocating more multidisciplinary studies of deception (Harrington, 2009).

We suggest that future research should include a more detailed analysis of the articles from the two clusters we identified as having the highest number of articles related to deception. This analysis would determine which articles are specifically focusing on deception, and how representative they are of the broader cyber-deception literature. Upon identifying a representative body of a specific and focused cyber-deception literature, a full set of scientometric analyses can be conducted to learn the keyword terms used in cyber-deception research, key concepts and themes, research approaches, and key researchers and co-author networks, and centers of cyber-deception research. In turn, these details from the core literature of cyber-deception research can then be mapped to the corresponding categories in the literature of classic deception research (e.g., Lorber & Stech 2009) to thus identify gaps, overlaps, commonalities, and differences.

Second, we suggest that future work should include building a terminology bridge between the cyber-space and the deception domains. This effort could result in a process to identify and map the tools, techniques, and practices used by researchers, planners, and practitioners in these two domains.

Given the current importance of cyber-security and the possible threat of cyber-warfare, it is necessary to identify the research gaps in the emerging cyber-deception field by analyzing the cyber-space literature, and to address those gaps by developing a framework that includes a terminology bridge, which can serve as a foundation for facilitating the development of offensive and defensive cyber-deception tools, techniques, and practices that are grounded in the latest, most advanced science. Such mappings identify opportunities for fruitful cross-disciplinary deception and counter-deception research, and thereby help develop new knowledge in the cyber-deception and counter-deception domains.

5. Acknowledgments

This work was funded internally by The MITRE Corporation.

6. References

Buller, D. B., & Burgoon, J. K. (1994). Deception: Strategic and Nonstrategic Communication. In J. A. Daly & J. M. Wieman (Eds.), *Strategic Interpersonal Communication* (pp. 191-223). Hillsdale, NJ, England: Lawrence Erlbaum Associates.

Coleman, L., & Kay P. (1981). Prototype Semantics: the English Verb Lie. *Language*, *57*(1), 26-44.

Daniel, Donald. C., & Herbig, Katherine. L. (1982). Propositions on Military Deception. In *Strategic Military Deception*, Ed. by Daniel, DC & Herbig, K.L. New York: Pergamon Press.

Deception Research Program. (1979). Misperception Literature Survey. Washington, DC: Office of Research and Development, Central Intelligence Agency.

Ekman, P. (1985). *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*. New York: W.W. Norton.

Ekman, P., & Friesen, W. V. (1969). The Repertoire of Nonverbal Behavior: Categories, Origins, Usage, and Coding. *Semiotica*, *1*, 49-98.

Epstein, E. J. (1989). *Deception: The Invisible War Between the KGB and the CIA*. New York: Simon and Schuster.

Glänzel, W. (2010). On reliability and robustness of scientometrics indicators based on stochastic models. An evidence-based opinion paper. *Journal of Informetrics*, *4*(3), 313-319. doi:10.1016/j.joi.2010.01.005

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Garden City: Doubleday Anchor.

Goffman, E. (1974). *Frame Analysis*. Boston: Northeastern University Press.

Harrington, B. (2009). *Deception: From Ancient Empires to Internet Dating.* Stanford University Press.

Heuer, R. J. (1981). Strategic Deception and Counter-Deception: A Cognitive Process Approach. *International Studies Quarterly*, *25*(2), 294-327.

Heuer, R. J. (1982). Cognitive Factors in Deception and Counter-Deception. In D. C. Daniel & K. L. Herbig (Eds.), *Strategic Military Deception* (pp. 155-177). New York: Pergamon Press.

Hopper, R., & Bell, R. A. (1984). Broadening the Deception Construct. *Quarterly Journal of Speech, 70*, 288-302.

Hyman, R. (1989). The Psychology of Deception. *Annual Review of Psychology, 40*, 133-154.

Lorber, M., & Stech, F. J. (2009). Scientometrics Study on Educing Information. *MITRE Technical Report* MTR090282, August 2009.

Masip, J., Garrido, E., & Herrero, Ca. (2004). Defining Deception. *Anales de Psycologia*, *20*(1), 147-171.

National Research Council. (1991). *In the Mind's Eye: Enhancing Human Performance*. Washington, DC: National Academy Press.

Ramachandran, V. S., & Rogers-Ramachandran, D. (1996). Synaesthesia in Phantom Limbs Induced with Mirrors. *Proceedings: Biological Sciences*, *263*(1369), 377-386.

Saarni, C. (1982). Social and Affective Functions of Nonverbal Behavior: Developmental Concerns. In R. S. Feldman (Ed.), *Development of Nonverbal Behavior in Children* (123-147). New York: Springer-Verlag.

Thompson, P. (2004). Cognitive hacking and intelligence and security informatics. Paper presented at the Enabling Technologies for Simulation Science VII, 13-15 April 2004, USA.

Whaley, B. (1982). Toward a General Theory of Deception. *The Journal of Strategic Studies, 5,* 178-192.

Yuill, J., Denning, D., & Feer, F. (2006). Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques. *Journal of Information Warfare, 5(3)*, 26-40. Retrieved from http://faculty.nps.edu/dedennin/publications/HidingFromHackers-JIW%205_3.pdf

Appendix A. Selected key characteristics for broad search “deception” related clusters

Key cluster characteristics (keywords, abstract phrases, authors, and journal titles) for the two “deception” related clusters (Cluster 19 and 7) are shown below. These tables show the most relevant cluster characteristics based on frequency within the cluster (shown as FGE). FGE stands for “frequency greater than or equal to” a particular number. Some cluster characteristics are not included based on their lack of relevance or uniqueness. For example, while the phrase “study” appeared in 43 abstracts, it does not describe a unique aspect of the cluster. The acronym FGE stands for "frequency greater than or equal to" a particular number. These are shown below for Cluster 19 and Cluster 7, the two "deception" related clusters.

Frequency	*Keyword*
21	security of data
16	psychology
14	computer crime
13	decision making
13	Internet
12	deception
12	linguistics
12	Social aspects
11	mathematical models
10	artificial intelligence
10	communication systems
10	feature extraction

Table A-1. Cluster 19 Keywords with FGE (10).

Frequency	*Abstract Phrase*
132	deception
44	deception detection
26	research
23	detection
22	analysis
22	information
18	humans
18	method
15	system
14	cues
14	methods
14	participants
14	truth
13	ability

13	development
13	messages
13	problem
12	deceivers
12	process
11	accuracy
11	individuals
11	knowledge
11	lies
11	systems
10	computer-mediated communication

Table A-2. Cluster 19 Abstract Phrases with FGE (10).

Frequency	***Journal***
5	Nature
4	Communications of the ACM
4	Decision Support Systems
4	Journal of Management Information Systems
3	Computers in Human Behavior
3	Journal of Forensic Sciences
3	Journal of Scientific Exploration
3	Trends in Cognitive Sciences

Table A-3. Cluster 19 Journal Titles with FGE (3).

Frequency	***Author***
34	Burgoon, Judee K
28	Nunamaker Jr, Jay F
14	George, Joey F
14	Twitchell, Douglas P
14	Zhou, Lina
9	Jensen, Matthew L
7	Adkins, Mark
6	Biros, David P
6	Kruse, John

Table A-4. Cluster 19 Authors with FGE (6).

On my way: Deceptive texting and interpersonal awareness narratives
Who stole the bat? Deception detection on the basis of actions
2010 ACM Conference on Computer Supported Cooperative Work, CSCW 2010
3D tactics and information deception
A Bayesian analysis of surveillance attribute data
A child's story to illustrate automated reasoning systems using opportunity and history
A comparison of classification methods for predicting deception in computer-mediated communication
A computational model for financial reporting fraud detection

A longitudinal analysis of language behavior of deception in e-mail
A method based on the rough neural network for analysing deception risks
A model of deception during cyber-attacks on information systems
A multi-layer Naive Bayes model for approximate identity matching
A multinomial-Dirichlet model for analysis of competing hypotheses
A probabilistic model for approximate identity matching
A quasi-experiment to determine the impact of a computer based deception detection training system: The use of Agent99 trainer in the U.S. military
A statistical language modeling approach to online deception detection
A study of glottal waveform features for deceptive speech classification
A study on deception detection based on classification for Chinese text
A system and method for enhanced psychophysiological detection of deception
A system and method for enhanced psychophysiological detection of deception, assured client verification with remote processing
A trust based information dissemination model for evaluating the effect of deceptive data
Advanced scientific detection of deception-ERP augmented polygraphy
Advances in automated deception detection in text-based computer-mediated communication
An Application of Deception in Cyber-space: Operating System Obfuscation
An approach for intent identification by building on deception detection
An Automated Process for Deceit Detection
An empirical investigation of deception behavior in instant messaging
An empirical study on dynamic effects on deception detection
An exploratory study into deception detection in text-based computer-mediated communication
An exploratory study on promising cues in deception detection and application of decision tree
An interactive system for generating arguments in deceptive communication
An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering
An ontology-supported misinformation model: Toward a digital misinformation library
Apoptosis: death deceiver
Applying poker strategies, tactics and rapid decision making methods to military decision making on the tactical level
Association rule mining for suspicious email detection: a data mining approach
Automated determination of the veracity of interview statements from people of interest to an operational security force
Automated high-level reasoning for deception detection: Two scenarios demonstrated
Automated linguistic analysis of deceptive and truthful synchronous computer-mediated communication
Automated stress detection using keystroke and linguistic features: An exploratory study
Automatic extraction of deceptive behavioral cues from video
AUTOMATIC SPEAKER VERIFICATION USING CEPSTRAL MEASUREMENTS
Automatically detecting deceptive criminal identities
BAYESIAN ANALYSIS OF SURVEILLANCE ATTRIBUTE DATA
Bayesics
Before Jane Goodall, there was Nadia Kohts

Behavioural and functional anatomical correlates of deception in humans
BELIEF REPRESENTATION FOR UNDERSTANDING DECEPTION
Beyond terms: multi-word units in multiterm extract
Blob analysis of the head and hands: A method for deception detection
Border Security Credibility Assessments via Heterogeneous Sensor Fusion
Bumble bees (Bombus terrestris) store both food and information in honeypots
Can online behavior unveil deceivers? - an exploratory investigation of deception in instant messaging
Charting the behavioural state of a person using a backpropagation neural network
ChatTrack: Chat room topic detection using classification
Colony nutritional status modulates worker responses to foraging recruitment pheromone in the bumblebee Bombus terrestris
Combining prosodic lexical and cepstral systems for deceptive speech detection
Comparison of computer programs designed to evaluate psychophysiological detection of deception examinations
Computer-based training for deception detection: What users want
Cooperation and Deception Recruit Different Subsets of the Theory-of-Mind Network
Cross-cultural deception in social networking sites and face-to-face communication
Cues to deception in online Chinese groups
CyberGate: a design framework and system for text analysis of computer-mediated communication
Cyberinfrastructure for homeland security: Advances in information sharing, data mining, and collaboration systems
DAWS: Denial and Deception Analyst Workstation
Deception across cultures: Bottom-up and top-down approaches
DECEPTION BY PENETRANTS
Deception detection based on SVM for Chinese text in CMC
Deception detection through automatic, unobtrusive analysis of nonverbal behavior
Deception detection under varying electronic media and warning conditions
Deception detection via blob motion pattern analysis
Deception discovery and employment with linguistic geometry
Deception in cyber-space: a comparison of text-only vs. avatar-supported medium
Deception used for cyber-defense of control systems
Deception: Toward an Individualistic View of Group Support Systems
Deceptive communication in virtual communities
Deceptive detection methods for effective security with inadequate budgets: The testing power index
Deceptive schedules: What can we do about them
Decision structuring with phantom alternatives
Decision support for determining veracity via linguistic-based cues
Delusion and deception in large infrastructure projects: two models for explaining and preventing executive disaster
Design and analysis of anti spamming SMS to prevent criminal deception and billing froud: case Telkom Flexi
Detecting Concealment of Intent in Transportation Screening: A Proof of Concept
Detecting deception in person-of-interest statements
Detecting deception in secondary screening interviews using linguistic analysis

Detecting deception in synchronous computer-mediated communication using speech act profiling
Detecting deception in testimony
Detecting deception in the brain: a functional near-infrared spectroscopy study of neural correlates of intentional deception
Detecting deception using critical segments
Detecting deception: the scope and limits
Detection of Deception in Structured Interviews Using Sensors and Algorithms
Detection of deception: Collaboration systems and technology
Determining the strength of a decoy system: a paradox of deception and solicitation
Developing group decision support systems for deception detection
Different patterns of cerebral activation in genuine and malingered cognitive effort during performance on the Word Memory Test
Distributed deception: an investigation of the effectiveness of deceptive communication in a computer-mediated environment
Distrusting online: Social deviance in virtual teamwork
Don't be fooled by bayes
Dorsolateral prefrontal cortex specifically processes general - but not personal - knowledge deception: Multiple brain networks for lying
Effects of computer-based instruction on student learning of psycho-physiological detection of deception test question formulation
Enabling Technologies for Simulation Science IX
Erratum: Seeing through the face bee of deception (Nature (2002) 415 (35
ESP: psychic perception-or deception
Evaluation of the NITV CVSA
Evolutionary biology. A case of self-deception
Expanding a catalogue of deceptive linguistic features with NLP technologies
Experience based reasoning for recognising fraud and deception
Exploration of feature selection and advanced classification models for high-stakes deception detection
Exploring the core concepts of media richness theory: The impact of cue multiplicity and feedback immediacy on decision quality
Eye movements and pupil size reveal deception in computer administered questionnaires
Facial deception in humans and ECAs
Facilitating benign deceit in mediated communication
Facing up to deception
Features of computer-mediated, text-based messages that support automatable, linguistics-based indicators for deception detection
Finding logically consistent resource-deception plans for defense in cyber-space
Following linguistic footprints: Automatic deception detection in online communication
Functional MRI Detection of Deception After Committing a Mock Sabotage Crime
Gender differences in deception and its detection under varying electronic media conditions
Generating nonverbal indicators of deception in virtual reality training
Goals, arguments, and deception: a formal representation from the Aurangzeb project. I: an episode from the succession war
Goals, arguments, and deception: A formal representation from the Aurangzeb project. II: A formalism for the capture of Murad

Heuristics and modalities in determining truth versus deception
HMM-based deception recognition from visual cues
How floral odours are learned inside the bumblebee (Bombus terrestris) nest
How novelty search escapes the deceptive trap of learning to learn
Hyperscanning: Simultaneous fMRI during linked social interactions
i2i trust in videoconferencing
Identification and doing it without IT, III: authoritative opinions, purposeful action, relabeled goods, and forensic examinations. The case of the stuffed birds: its narrative dynamic set in formulae
Identification and doing without it, III: Authoritative opinions, purposeful action, relabeled goods, and forensic examinations. The case of the stuffed birds: Its narrative dynamics set in formulae
Identification of deceptive behavioral cues extracted from video
Identification of deliberately doctored text documents using frequent keyword chain (FKC) model
Impossibility of deception in a conflict among subjects with interdependent preference
Improving a textual deception detection model
Inconsistency in deception for defense
Inducing sensitivity to deception in order to improve decision making performance: a field study
Information, decision-making and deception in games
Inhibiting deception and its detection
Interactions between system evaluation and theory testing: A demonstration of the power of a multifaceted approach to information systems research
Investigating the use of a Bayesian Network to model the risk of Lyngbya majuscula bloom initiation in deception bay, Queensland, Australia
Judging the credibility of information gathered from face-to-face interactions
Language dominance in interpersonal deception in computer-mediated communication
Lie tracking: Social presence, truth and deception in avatar-mediated telecommunication
Lie-specific involvement of dorsolateral prefrontal cortex in deception
Lie-Truth Allometric Power Law Modeling and Brain Chemistry Simulation Verification
Making it hard to lie: Cultural determinants of media choice for deception
Managing deceitful reports with the transferable belief model
Masters of deception
Mate Choice Models - Can Cost of Searching and Cost of Courtship Explain Mating Patterns of Female Pied Flycatchers
Media selection for deceptive communication
Mental states in animals: Cognitive ethology
Method for military deception planning
Methodologies for deception detection based on abnormal behavior
Midway revisited: Detecting deception by analysis of competing hypotheses
Modality effects in deception detection and applications in automatic-deception-detection
Modeling and handling uncertainty in deception detection
Modeling deceptive information dissemination using a holistic approach
Modeling self-deception within a decision-theoretic framework
Motion Profiles for Deception Detection Using Visual Cues

Moving toward intent detection: A tool-based approach
Networks of gene regulation, neural development and the evolution of general capabilities, such as human empathy
Neural correlates of telling lies: A functional magnetic resonance imaging study at 4 Tesla
Neural Network Evaluation of Multi-Modal Startle Eyeblink Measurements
Neural processes underlying self- and other-related lies: An individual difference approach using fMRI
Neuroscience, lie-detection, and the law. Contrary to the prevailing view, the suitability of brain-based lie-detection for courtroom or forensic use should be determined according to legal and not scientific standards
Nonverbal indicators of malicious intent: affective components for interrogative virtual reality training
Note on the role of deception in information protection
Novel cybermatic medical communication system (CMCS
Oligopoly limit pricing
On a text-processing approach to facilitating autonomous deception detection
On deception detection in multi-agent systems and deception intent
On deception detection in multiagent systems
On detecting deception in agent societies
Painful deception [2] (multiple letters
Personality factors in human deception detection: Comparing human to machine performance
Phoretic nest parasites use sexual deception to obtain transport to their host's nest
Polygyny in the pied flycatcher (Ficedula hypoleuca): comparison of deception and non-deception models
Potential noncontact tools for rapid credibility assessment from physiological and behavioral cues
PRM-based identity matching using social context
Proceedings of SPIE - Nondestructive Detection and Measurement for Homeland Security III
Protection against deception - Generally accepted product labelling in the light of the amended labelling directive
Purported anomalous perception in a highly skilled individual: Observations, interpretations, compassion
Quantitative analysis of American deceive strategies in the Gulf War
Reading between the lines: Linguistic cues to deception in online dating profiles
Religion's evolutionary landscape: counterintuition, commitment, compassion, communion
Renormalizable `deception' theory of weak interactions
Representation and reasoning under uncertainty in deception detection: a neuro-fuzzy approach
Research on active network defense technology based on deception
Research on credit card fraud detection model based on similar coefficient sum
Robot deception: recognizing when a robot should deceive
ROLE OF GOLD IN ALCHEMY. PART III
Safety from deception through broadband coding The Austrian victory over the hackers at Graz in 1991
Sarcasm, deception, and stating the obvious: planning dialogue without speech acts

Secrets and lies in computer-mediated interaction: Theory, methods and design
Security protection design for deception and real system regimes: A model and analysis
Seeing through the face of deception
Self-deception and emotional coherence
Seven Deadly Hiring Mistakes: Beware, some people are masters of deception
Sexual Recombination in Self-Organizing Interaction Networks
Six patterns for persuasion in online social networks
Social desirability and controllability in computerized and paper-and-pencil personality questionnaires
Speech act profiling: a probabilistic method for analyzing persistent conversations and their participants
Speech analysis using modulation-based features for detecting deception
Storming and forming a normative response to a deception revealed online
Suspicious e-mail detection via decision tree: a data mining approach
Symantec deception server experience with a commercial deception system
Task complexity and deception detection in a collaborative group setting
Task performance under deceptive conditions: Using military scenarios in deception detection research
Technology dominance in complex decision making: The case of aided credibility assessment
Technology of deception
Testing various modes of computer-based training for deception detection
The \`deception' of code smells: An empirical investigation
The automatic prevention and control research of ARP deception and implementation
The Chemistry of Sexual Deception in an Orchid-Wasp Pollination System
The cognitive processes related to deceptive responding
The cybernetics of lying
The deceptive behaviors that OFFEND us MOST about Spyware
The effect of deception on optimal decisions
The effects of warnings, computer-based media, and probing activity on successful lie detection
The impact of media richness, suspicion, and perceived truth bias on deception detection
The motivational enhancement effect: Implications for our chosen modes of communication in the 21st century
The puzzling science of information integrity
The Soviet Army-armor and electronics
The undergrowth of science: Deception, self-deception, and human frailty by Walter Gratzer
Thermal facial screening for deception detection
Think-tank calls for an end to DNA deception
Time-domain analysis of EEG during guilty knowledge test: investigation of epoch extraction criteria
To deceive or not to deceive: the effect of deception on behavior in future laboratory experiments
Toward detecting deception in intelligent systems
Towards deceptive intention: Finding trajectories and its analysis
Training to detect deception: an experimental investigation
Trust and deception in mediated communication

Truth, lies, reality and deception: An issue for e-commerce
Types of deception and underlying motivation - What people think
Typing or messaging? Modality effect on deception detection in computer-mediated communication
UK Royal Navy to field AIS deception capability
Unusual Suspects: Fish gotta fib, birds gotta lie. But when animals deceive, do they know what their dupes are thinking
User experience with Agent99 Trainer: a usability study
User experiences with an unobtrusive decision aid for deception detection
Using a cognitive architecture to automate cyberdefense reasoning
Using a linguistic analysis tool to detect deception
Using brain MERMER testing to detect knowledge despite efforts to conceal
Using linguistic cues for the automatic recognition of personality in conversation and text
Using speech act profiling for deception detection
Vallee comments on book review 'revelations. Alien contact and human deception
Very idea of computer self-knowledge and self-deception
Video surveillance and human activity recognition for anti-terrorism and force protection
Virtual humans with secrets: Learning to detect verbal cues to deception
Warrants and deception in computer mediated communication
Weapons of Mass Deception (WMD): Fibs, lies ambiguities
Weapons of mass deception [virus trapping
Worst-case sensing deception in cognitive radio networks
Writeprints: A stylometric approach to identity-level identification and similarity detection in cyber-space

Table A-5. Cluster 19 Article Titles.

Frequency	***Keyword***
48	multi-agent systems
40	game theory
37	software agents
29	Internet
28	security of data
27	electronic commerce
21	multi agent systems
20	decision making
19	computer crime
18	mathematical models
15	artificial intelligence
15	computer simulation
14	algorithms
13	computer games
13	probability
13	problem solving
10	inference mechanisms
10	intelligent agents

Table A-6. Cluster 7 Keywords with FGE (10).

Frequency	*Abstract Phrase*
70	agents
65	deception
37	agent
34	trust
30	approach
26	information
23	system
20	method
17	game
17	Internet
16	problem
15	reputation
14	cooperation
13	interaction
13	systems
12	application
12	behavior
12	environment
12	game theory
11	knowledge
11	mechanism
11	players
11	simulation results
11	trustworthiness
10	analysis
10	basis
10	development
10	effects
10	fraud
10	games
10	group
10	quality

Table A-7. Cluster 7 Abstract Phrases with FGE (10).

Frequency	*Journal*
3	Applied Artificial Intelligence
3	Science in China Series F-Information Sciences
2	Computational Intelligence
2	Ieice Transactions on Information and Systems
2	International Journal of Computer Games Technology
2	International Journal of Electronic Commerce
2	Management Science
2	Science China-Information Sciences
2	Service Oriented Computing and Applications

Table A-8. Cluster 7 Journals with FGE (2).

Frequency	***Author***
4	Castelfranchi, C
4	Singh, Rajdeep
3	Kotenko, I
3	Krishnaswamy, Shonali
3	Loke, Seng W
3	Maithripala, D. H. A
3	Sen, S
3	Sherchan, Wanita
3	Tambe, M

Table A-9. Cluster 7 Authors with FGE (3).

2004 IEEE 1st Symposium on Multi-Agent Security Survivability
3D Cyberpuck - excellent smooth scrolling action
A BDI agent architecture for reasoning about reputation
A cognitive approach to intrusion detection
A computation trust model with trust network in multi-agent systems
A coordination strategy for cooperative sensor network deception by autonomous vehicle teams
A deceit-tolerant negotiation model for agent mediated electronic commerce
A direct reputation model for VO formation
A formal framework for user centric control of probabilistic multi-agent cyber-physical systems
A fully abstract encoding of the pi-calculus with data terms (Extended abstract
A fuzzy model for reasoning about reputation in web services
A fuzzy multi-criteria decision model for information system security investment
A game of deception
A game theoretic approach for quantitative evaluation of security by considering hackers with diverse behaviors
A game theoretic approach for quantitative evaluation of strategic interactions between hacker's motivations
A learning-enabled integrative trust model for e-markets
A model of deceit-tolerant automated negotiation for open environment
A Multi-agent Model of Deceit and Trust in Intercultural Trade
A new decision-making approach for C2C electronic trade
A new dynamic defense model based on active deception
A novel approach to manage trust in ad hoc networks
A realistic chat environment for virtual avatars in cyber-space
A reputation management system model for e-commerce community
A reputation-based market model in grid environment
A reputation-based service selection scheme
A robust deception-free coalition formation model
A security-based agent for a virtual enterprise
A study of cooperative work support in the CyberOffice
A study on cyber-campus community using mobile agents
A warm cyber-welcome: using an agent-led group tour to introduce visitors to Kyoto
Abstracting and verifying strategy-proofness for auction mechanisms
Accounting for the human in cyber-space: Effects of mood on trust in automation
Acquaintance-based trust model for the evolution of cooperation in business games
Active mechanism of deceit detection for multi-agent based interaction
Adaptive Markov game theoretic data fusion approach for cyber-network defense
Adversarial problem solving: modeling an opponent using explanatory coherence
Adversarial reasoning: challenges and approaches
Agent teams in cyber-space: security guards in the global Internet
Agent-Based Approach to Conforming Behavior Analysis in a Cyber-Market
Agent-based collaboration between distributed web applications: Case study on "collaborative design for X" using CyberCO
Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in Internet

Agent-based user-profiling model for behavior monitoring
Agent-oriented public key infrastructure for multi-agent e-service
Algorithmic mechanisms for internet-based master-worker computing with untrusted and selfish workers
An adaptive reputation model for VOs
An agent based privacy preserving mining for distributed databases
An approach for detecting deception in agents
An axiomatic basis for reasoning about trust in PKIs
An enhancement of the random sequence 3-level obfuscated algorithm for protecting agents against malicious hosts
An evolutionary approach to deception in multi-agent systems
An improved trust model based on reputation in P2P networks
An intelligent agent-based collaborative information security framework
An intelligent agent-based framework for collaborative information security
An intelligent proactive security system for cyber centres using cognitive agents
Analyze and guess type of piece in the computer game intelligent system
Architecture for cyber command and control: experiences and future directions
Artificial liars: why computers will (necessarily) deceive us and each other
Assimilation and survival in cyber-space
Auction-based spectrum sharing for multiple primary and secondary users in cognitive radio networks
Automated Social Coordination Of Cyber-physical Systems With Mobile Actuator And Sensor Networks
Automated trading in agent-based markets for communication bandwidth
Bayesian reputation modeling in E-marketplaces sensitive to subjectivity, deception and change
Believing others: pro and cons
Believing others: Pros and cons
Both-branch fuzzy decision and decision encryption-authentication
Building dynamic agent organizations in cyber-space
Can computers deliberately deceive? - A simulation tool and its application to Turing's imitation game
Can computers deliberately deceive? A simulation tool and its application to turing's imitation game
Catch me if you can - Exploring lying agents in social settings
Challenge of trust, The Autonomous Agents '98 Workshop on Deception, Fraud and Trust in Agent Societies
Challenges for trust, fraud and deception research in multi-agent systems
Cluster-based analysis and recommendation of sellers in online auctions
Collaborative diffusion: Programming antiobjects
Combinatorial games
Combining trust and reputation management for Web-based services
Computing in pervasive cyber-space
Coping with deception
Corporate knowledge in cyberworlds
Counterplanning deceptions to foil cyber-attack plans
Cyber agent on the World Wide Web
Cyber games and interactive entertainment
CyberAgent: Collaborative agents for distributed applications over the internet
CyberCromlech: a new framework for collective behaviour game experiments
Cybernetic behaviour of the intelligent agent ConRaider. Application to the computer-assisted maintenance
Cyberoos'2001: "Deep behaviour projection" agent architecture
Cyberoos'99: tactical agents in the RoboCup Simulation League
CyberRescue: a pheromone approach to multi-agent rescue simulations
Cyber-space WWW EC authenticated computing
Cyberwar plans trigger intelligence controversy
Cyberwar XXI quantifying the unquantifiable adaptive AI for next generation conflict simulations
Data-protection ordering/disordering of a fuzzy logic model in a robotic agent via the optical-data-transfer line
Deception games
Deception in autonomous vehicle decision making in an adversarial environment
Detecting cheaters for multiplayer games: Theory, design and implementation
Detecting deception in intelligent systems I: Activation of deception detection tactics

Detecting Deception in Reputation Management
Dynamic Bayesian approach for detecting cheats in multi-player online games
Dynamic Trust Model Based on Perceived Risk
Editorial: Cyber games and interactive entertainment
Effect of referrals on convergence to satisficing distributions
Emergence in cyber-space: towards the evolutionary self-organising enterprise
Emerging collective behavior in a simple artificial financial market
Entertainment on the PC: adventure, murder and data robbery
Epistemic formulae, argument structures, and a narrative on identity and deception: a formal representation from the AJIT subproject within AURANGZEB
Evolution of cooperativeness in a business game relying on acquaintance based trustworthiness assessment
Experiences with DREGS
Experiments on robustness and deception in a coalition formation model
Explanation-aware service selection: Rationale and reputation
Extension of hypergame analysis and its application
Extension of the LG hypergame to "inner games" played over the topology of competing "mind nets
Feasibility considerations in formation control: phantom track generation through multi-UAV collaboration
Feasibility of multi-agent simulation for the trust and tracing game
Finding and moving constraints in cyber-space
Finding exploratory rewards by embodied evolution and constrained reinforcement learning in the cyber rodents
Foraging for information resources in cyber-space: intelligent foraging agent in a distributed network
Fraud detection in reputation systems in e-markets using logistic regression
Fuzzy approach for the evaluation of trust and reputation of services
Fuzzy referral based cooperation in social networks of agents
Game analysis and prevention mechanism for food quality supervision collusion
Game mods: customizable learning in a K16 setting
Game theoretic approach to threat prediction and situation awareness
Games of deception
Hack, slash, and chat: A study of players' behavior and communication in MMORPGs
Hacked devices, a new game experience, and a Wi-Fi detector shirt
Hohfeld in cyber-space and other applications of normative reasoning in agent technology
How trade partners make their decision in cyber-space: a research based on stochastic games
Hypergame Theory applied to Cyber Attack and Defense
Immune system based multi-agent information security system
Improved strategies in merger and acquisition negotiations from a bargaining model
In praise of forgiveness: ways for repairing trust breakdowns in one-off online interactions
In pursuit of peace: attitudinal and behavioral change with simulations and multiple identification theory
Incomplete information and deception in multi-agent negotiation
Information security with formal immune networks
Integrating trust into the CyberCraft initiative via the trust vectors model
Intelligent agents
Intelligent cyber logistics using reverse auction in electronic commerce
Intelligent Multi-Agent based Back-Propagation Neural Network Forecasting Model for Statistical Database Anomaly Prevention System
Knowledge focus via software agents
La 'retro-action cybernetique' et un modele de temps discret dans le paradoxe d'Einstein, Podolsky et Rosen
LARKS: dynamic matchmaking among heterogeneous software agents in cyber-space
Learning to survive
Limiting deception in groups of social agents
Maximizing utility of mobile agent based E-commerce applications with trust enhanced security
MEBRS: A multiagent architecture for an experience based reasoning system
Message and/or transmitter authentication
Modeling secrecy and deception in a multiple-period attacker-defender signaling game
Multi agents in mid involvement deception systems
Multi-object auctions: sequential vs. simultaneous sales
Negotiations with inaccurate payoff values
Nested beliefs, goals, duties, and agents reasoning about their own or each other's body in the

TIMUR model: A formalism for the narrative of tamerlane and the three painters
NetGames 2004 workshop
New algorithms for mining the reputation of participants of online auctions
NSF activities in Cyber Trust
On a view model of agents in the cyber office
On the response policy of software decoys: Conducting software-based deception in the cyber battlespace
One-time key generation system for agent data protection
Ontology-based multi-agent model of an information security system
Opponent modeling in poker
Optimal Allocation of Resources for Defense of Simple Series and Parallel Systems from Determined Adversaries
Optimal authentication systems
ORTS: a hack-free RTS game environment
Phantom track generation in 3D through cooperative control of multiple ECAVs based on geometry
Phantom track generation through cooperative control of multiple ECAVs based on feasibility analysis
Poker as a testbed for AI research
Por favor? favor reciprocation when agents have private discounting
Practical theory and theory-based practice [agent based systems
Prevention, detection and recovery from cyber-attacks using a multilevel agent architecture
Principal-agent model for multi-agent cooperation
Proceedings of SPIE - Modeling and Simulation for Military Operations III
Proceedings of the 3rd international workshop on multi-agent robotic systems - mars 2007; in conjunction with ICINCO 2007
Prospectives for modelling trust in information security
Prospects of agents in cyber-space
Protecting e-commerce agents from defamation
Proving properties of open agent systems
Pursuit-evasion differential games with deception or interrupted observation
Qualitative trust modeling in SOA
Recursive agent and agent-group tracking in a real-time, dynamic environment
Regularity-based trust in cyber-space
Reputation evaluation model in grid-supported based on D-S evidence theory
Reputation-aware contract-supervised grid computing
Requirements for belief models in cooperative dialogue
Research on theory and key technology of trusted computing platform security testing and evaluation
Research on trusted computing and its development
Revising beliefs through arguments: bridging the gap between argumentation and belief revision in MAS
Robustness against deception in unmanned vehicle decision making
RRM: An incentive reputation model for promoting good behaviors in distributed systems
Simulation of multi-agent based cybernetic transportation system
Socio-cognitive mechanisms of belief change. Applications of generalized game theory to belief revision, social fabrication, and self-fulfilling prophesy
Some compartmentalized secure task assignment models for distributed systems
Strategic deception in agents
StrikeCOM: A multi-player online strategy game for researching and teaching group dynamics
Study of robot soccer attack path and action based on recursive algorithm
Substitution rules for the verification of norm-compliance in electronic institutions
Support of reflective mobile agents in a smart office environment
Survival in cyber-space
Swift trust in a virtual temporary system: A model based on the Dempster-Shafer theory of belief functions
Synchronization Properties of Cyber Behaviors
Teamwork in cyber-space: using TEAMCORE to make agents team-ready
Teamwork of hackers-agents: Modeling and simulation of coordinated distributed attacks on computer networks
Terraforming cyber-space
The challenge of poker
The control of teams of autonomous objects in the time-constrained environments

The Cyber Rodent Project: exploration of adaptive mechanisms for self-preservation and self-reproduction
The cybercraft system ontology: An ontology for reasoning about distributed agent capabilities
The deception detection and restraint in multi-agent system
The dynamics of trust in cyberdomains
The EigenRumor algorithm for calculating contributions in cyber-space communities
The ethics of deception: why AI must study selfish behaviour
The Hacker: new mythical content of narrative games
The handicap principle for trust in computer security, the semantic web and social networking
The intelligent vehicle coordination of the cybernetic transportation system
The physical body in cyber-space: at the edge of extinction
The role of trust and deception in virtual societies
Three key issues of multi-auctioneer model in computer grid
Three-player Hackenbush played on strings is NP-complete
Topical trustrank: Using topicality to combat web spam
Towards an extended evolutionary game theory with survival analysis and agreement algorithms for modeling uncertainty, vulnerability, and deception
Towards Deception in Agents
Towards explanation-aware selection in internet-scale infrastructures: Generating rationale for web services ratings and reputation
Trading in open marketplace using trust and risk
Trust-sensitive Web service composition strategy based on black and white board
Truth or consequences: An experiment
Unexceptional.net: a story about a unique pervasive game
Unmanned vehicle operations under imperfect information in an adversarial environment II
Unmanned vehicle operations: Countering imperfect information in an adversarial environment
Use of trust vectors for CyberCraft and the limits of usable data history for trust vectors
Using logic programming to detect deception on the basis of actions
Using the multi-living agent concept to investigate complex information systems
Using trust for detecting deceitful agents in artificial societies
Verifying dominant strategy equilibria in auctions
Winnowing wheat from the chaff: propagating trust to sift spam from the Web

Table A-10. Cluster 7 Article Titles.

Appendix B. Full-text extraction phrases and terms

Freq	*Phrase*	*Freq*	*Phrase*
266	United States	70	cyber-security
248	cyber-warfare	70	information system
242	air force	67	cyber-war
197	information warfare	67	human behavior
171	national security	66	control system
165	information systems	66	system designer
157	information technology	65	law enforcement
152	cyber-attacks	63	attack graph
146	face to face	63	social psychology
135	cyber-space operations	62	command and control
135	information operations	62	information assurance
128	information security	61	mediated communication
119	military deception	59	computer network
118	intrusion detection	59	media richness
103	computer mediated	59	South Korea
103	North Korea	56	computers in human
101	denial of service	55	computers in human behavior
100	computer security	55	electronic warfare

99	deception system	55	network security
96	cyber-attack	55	open source
89	critical infrastructure	54	protection level
87	Department of Defense	54	risk analysis
85	real system	54	risk management
83	computer networks	53	information technologies
82	cyber-deception	52	real time
80	information content	52	computer system
79	military operations	52	information visualization
77	computer systems	52	mildec operations
74	operating system	50	long term
72	private sector	50	armed forces
71	national defense	50	decision maker

Table B-1. Full-text Extraction Phrases and Terms (200).

Freq	*Phrase*	*Freq*	*Phrase*	*Freq*	*Phrase*
3440	information	382	adversary	257	operational
1746	deception	382	capabilities	257	trust
1744	security	376	air	254	training
1487	system	373	behavior	251	attackers
1440	cyber	372	planning	251	operation
1309	attack	371	online	250	action
1112	computer	371	study	250	communications
1080	systems	367	target	250	sector
1062	data	364	support	249	media
1010	operations	364	world	248	business
977	military	355	management	248	cyber-warfare
951	attacks	347	war	248	theory
921	network	320	critical	247	journal
908	time	314	knowledge	243	self
877	cyber-space	313	users	242	air force
844	internet	312	forces	242	related
770	research	309	development	240	ability
691	analysis	306	actions	240	key
678	warfare	304	command	240	specific
650	intelligence	300	potential	237	public
637	attacker	300	source	236	threats
618	national	299	order	235	problem
599	technology	298	design	234	domain
565	defense	297	computers	233	techniques
557	software	296	physical	232	electronic
550	government	294	tools	232	technologies
492	force	293	program	231	psychology
477	mildec	293	web	228	content
472	level	292	space	228	department
455	states	291	terrorism	228	individuals
451	control	289	international	226	code
448	access	287	risk	224	methods
445	figure	285	services	221	response
439	social	279	strategic	220	issues
437	model	278	paper	220	value
436	state	273	power	219	china
426	people	272	cost	219	common
425	university	272	groups	219	environment
413	process	272	report	217	DNS

406	communication	270	resources	217	policy
405	networks	269	general	217	relationships
404	human	267	case	214	organizations
404	real	267	organization	214	science
402	detection	266	United States	212	cognitive
400	joint	265	vulnerabilities	211	capability
398	protection	264	impact	211	studies
398	threat	261	hackers	209	Korea
397	group	260	plan	206	address
386	decision	259	activities	205	mission
385	infrastructure	259	Future	201	intrusion
385	user	259	strategy	200	servers

Table B-2. Full-text Extraction Terms with FGE (200).

Appendix C. SME-Identified cyber-deception literature

This appendix contains bibliographic citations for the set of 50 subject matter expert (SME)-identified cyber-deception literature. This set of literature was used for several analyses. The 22 bibliographic citations marked with an asterisk (*) denote the papers used for the cyber-deception terminology analysis. The full set of 50 papers was used in the full-text extraction analysis.

---Milestones in the history of information warfare (May 24, 2007). *The Economist*.

---A good bot roast (June 21, 2007). *The Economist*.

Bain, B. (Feb 18, 2010). Cyberattack simulation highlights vulnerabilities. *Government Computer News*. Retrieved from http://gcn.com/articles/2010/02/16/web-cybershockwave.aspx

Billo, C., & Chang, W. (2004). *Cyber Warfare: An Analysis of The Means And Motivations of Selected Nation States*. Dartmouth College, Institute for Security Technology Studies, Hanover, NH.

*Boyer, W. F., & McQueen, M. A. (2009). Deception used for Cyber Defense of Control Systems (No. INL/CON-08-15204): Idaho National Laboratory.

*Cilluffo, F. J., & Nicholas, J. P. (2006). Cyberstrategy 2.0. *The Journal of International Security Affairs, 10*, 27-31.

*Cohen, F. (1999). Simulating cyber attacks, defenses, and consequences. *Computers and Security*, *18*(6), 479-518.

Cohen, F. (2001). Should we use deception as an InfoSec defense? *Network Security*, 18-19.

Cohen, F. (2002). Protection by deception. *Network Security*, 17-19.

*Cohen, F., & Koike, D. (2003). Leading attackers through attack graphs with deceptions. *Computers & Security*, 22 (Copyright 2004, IEE), 402-411.

Commission on Behavioral and Social Sciences and Education (1991). Hiding and Detecting Deception. In D. Druckman & Bjork R. A. (Eds.), *The Mind's Eye: Enhancing Human Performance*. Washington, DC: National Academy Press.

*Conti, G., Ahamad, M., & Stasko, J. (2005). Attacking information visualization system usability overloading and deceiving the human. In *SOUPS '05 Proceedings of the 2005 symposium on Usable privacy and security* (p. 89-100). New York: ACM Press.

*Cornwell, B., & Lundgren, D. C. (2001). Love on the Internet: Involvement and misrepresentation in romantic relationships in cyberspace vs. realspace. *Computers in Human Behavior*, *17*(2), 197-211.

Cyberinfrastructure Council (2007). *Cyberinfrastructure vision for 21st century discovery.* Arlington, VA: National Science Foundation.

Defense Science Board (1996). Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D). Washington, D.C.

Derian, J.D. (1994). Cyber-Deterrence. *Wired Magazine*, 2. Retrieved from http://www.wired.com/wired/archive/2.09/cyber.deter.html

*Galanxhi, H., & Nah, F. F. H. (2007). Deception in cyberspace: a comparison of text-only vs. avatar-supported medium. *International Journal of Human-Computer Studies*, *65*, 770-783.

George, J. F., Biros, D. P., Adkins, M., Burgoon, J. K., & Nunamaker, J. F. (2004). Testing various modes of computer-based training for deception detection. In *Proceedings of Intelligence and Security Informatics, Second Symposium on Intelligence and Security Informatics, ISI 2004* (p. 411-417). Heidelberg: Springer-Verlag.

George, J. F., Biros, D. P., Burgoon, J., & Nunamaker, J. F. (2003). Training professionals to detect deception. In *ISI'03 Proceedings of the 1st NSF/NIJ conference on Intelligence and security informatics* (p. 366-370). Heidelberg: Springer-Verlag.

Gompert, D. C., & Kugler, R. L. (2006). Custer in Cyberspace. *Defense Horizons*, *51*, 1-11.

Hinde, S. (2005). Identity theft & fraud. *Computer Fraud & Security*, *6*, 18-20.

Joint Chiefs of Staff (2006). Military deception (No. Joint Publication 3-13.4 (formerly JP3-58)). Washington, D.C.: Department of Defense.

Jones, J. D., Joshi, H., Topaloglu, U., & Nelson, E. (2008). *Sherlock Holmes goes Cyber: Deception Detection on the Basis of Actions.* Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.88.1595&rep=rep1&type=pdf

*Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, *25*(7), 522-538.

*Kramer, F. D., Starr, S. H., Wentz, L., Zimet, E., & Kuehl, D. (2007). Frameworks and Insights Characterizing Trends in Cyberspace and Cyberpower. Paper presented at the *12th ICCRTS, Adapting C2 to the 21st Century*.

Lawson, S. (2001). The cyber-intifada: activism, activism, and cyber-terrorism in the context of the "New Terrorism". Unpublished Seminar paper for the course in Information Warfare and Security, taught by Dorothy Denning, Georgetown University.

Lemos, R., & McCullagh, D. (2002). Cybersecurity plan lacks muscle. *CNet News.com.* Retrieved from http://news.com.com/2102-1023_3-958545.html?tag=st_util_print

*Lynn, W. F. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, *89*(5), 97-108.

Montgomery, M. C. (2000-Spring). Cyber Threats: Developing a National Strategy for Defending Our Cyberspace. Paper presented at the *Seminar on Intelligence Command and Control,* Cambridge, MA, USA.

*Mulvenon, J. (2005). Toward a cyberconflict studies research agenda. *IEEE Security and Privacy*, 3(4), 52-55.

National Science Foundation *Cyberinfrastructure Research for Homeland Security: NSF Workshop Report.* Arlington, VA: National Science Foundation.

Neilson, R. E. (Ed.) (2003). *Sun Tzu and Information Warfare: A collection of winning papers from the Sun Tzu Art of War in Information Warfare Competition*. Washington, DC: National Defense University Press.

*Papadimitriou, F. (2009). A nexus of Cyber-Geography and Cyber-Psychology: Topos/"Notopia" and identity in hacking. *Computers in Human Behavior*, *25*, 1331-1334.

Parang, E. (2003). Web of Deception: Misinformation on the Internet [book review]. *Serials Review*, *28*(3)*,* 65-68.

Patterson, T. (2010). Inside the Pentagon's cyber war games. *Government Computer News*. Retrieved from http://gcn.com/Articles/2010/10/07/Inside-Pentagon-cyber-war-game.aspx?Page=1&p=1

*Piazza, J., & Bering, J. M. (2009). Evolutionary cyber-psychology: Applying an evolutionary framework to Internet behavior. *Computers in Human Behavior*, *25*(6), 1258-1269.

President's Information Technology Advisory Committee (2005). Cyber Security: A Crisis of Prioritization, *National Coordination office for Information Technology Research and Development.* Arlington, VA, USA.

*Rockmann, K. W., & Northcraft, G. B. (2008). To be or not to be trusted: The influence of media richness on defection and deception. *Organizational Behavior and Human Decision Processes*, *107*(2)*,* 106-122.

Rowe, N. (2007). Planning Cost-Effective Deceptive Resource Denial in Defense to Cyber-Attacks, In *Proceedings of ICIW 2007 Proc. 2nd International Conference on Information Warfare* (p. 177-184). Perth: Edith Cowan University.

Rowe, N. C. (2003-June). Counterplanning deceptions to foil cyber-attack plans. Paper presented at the *IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*. West Point, New York, USA.

*Ryu, C., Sharman, R., Rao, H. R., & Upadhyaya, S. (2010). Security protection design for deception and real system regimes: A model and analysis. *European Journal of Operational Research*, *201*(2), 545-556.

Shimeall, T., Williams, P., & Dunlevy, C. (2001). Countering cyber war. *NATO review*, *49*(4), 16-28.

Tan, K. L. (2003). *Confronting Cyberterrorism with Cyber Deception*. Naval Postgraduate School, Monterey, CA.

Terry, J. P. (2000). Cyberspace and the use of force. *Duke Journal of Comparative & International Law*, *9*, 491-494.

Thomas, T. L. (1996). Deterring information warfare: a new strategic challenge. *Parameters*, *26*, 81-91.

Thomas, T. L. (2008). Cyberskepticism: The mind's firewall. *IOSphere*, Spring, 4-8.

*Thompson, P. (2004-April). Cognitive hacking and intelligence and security informatics. Paper presented at *Enabling Technologies for Simulation Science VII*, USA.

*Thompson, P. *Utility-Theoretic Information Retrieval, Cognitive Hacking, and Intelligence and Security Informatics.* Dartmouth College, Hanover, NH, retrieved from http://www.ists.dartmouth.edu/library/77.pdf

*Thompson, P., & Giani, A. (2007 – May). *Detecting Deception in the context of Web 2.0.* Paper presented at Web 2.0 Security & Privacy, Oakland, CA. Retrieved from http://w2spconf.com/2007/papers/paper-212-z_6165.pdf

*Tinnel, L. S., Saydjari, O. S., & Farrell, D. (2002). Cyberwar Strategy and Tactics. Paper presented at *the 2002 IEEE Workshop on Information Assurance United States Military Academy*. West Point, New York, USA.

*Tirenin, W., & Faatz, D. (1999). A concept for strategic cyber defense. *Military Communications Conference Proceedings.* MILCOM 1999. *IEEE, 1,* 458-463.

Van Heuven, M., Botterman, M., De Spiegeleire, S., & Europe, R. (2003). *Managing New Issues: Cyber Security in an Era of Technological Change*. Santa Monica, CA: RAND.

Ware, W. H. (1998). *The cyber-posture of the national information infrastructure.* Santa Monica, CA: RAND.

*Whitty, M. T., & Carville, S. E. (2008). Would I lie to you? Self-serving lies and other-oriented lies told across different media. *Computers in Human Behavior*, *24*(3), 1021-1031.

*Yuill, J., Wu, F., Settle, J., Gong, F., Forno, R., Huang, M., et al. (2000). Intrusion-detection for incident-response, using a military battlefield-intelligence process. *Computer Networks-the International Journal of Computer and Telecommunications Networking*, *34*(4), 671-697.