Drexel’s Cybersecurity Institute (DCI) made great strides forward in 2015 on three fronts: research, teaching, and community engagement.

**Research:** Drexel cybersecurity research made great strides this year in several categories, including several new federal and corporate grants, a wide array of research proposal submissions, articles published in top-tier conferences and journals, successful defenses of several Ph.D. students, leadership in and engagement with the cybersecurity research community, and continued steps toward technology commercialization.

**Teaching:** Drexel cybersecurity education also made great strides this year in several categories, including several new courses, our first group of students graduating with the MS in Cybersecurity degree, fruitful engagement with Drexel University online, a new partnership with the U.S. Army Reserve on cybersecurity education, engagement with the College of Engineering Peace Engineering initiative, and many others.

**Community engagement:** DCI continued its commitment to meaningful engagement with the community by giving several invited talks, and organizing or co-organizing a number of symposia, invited lectures, and events on campus. In addition, DCI hosted its the inaugural meeting of its external advisory board in March, receiving strategic guidance from cybersecurity thought leaders.

Finally, I wish to extend my personal thanks to Norm Balchunas, our Operations Director until July of this year, for his tireless efforts in launching the DCI. His energy and leadership were instrumental in getting the Institute up and running over its first eighteen months.

This document summarizes Drexel University cybersecurity-related activities in 2015. Activities are broken down into the following categories:

1. Research activities
2. Business development activities
3. Educational activities
4. Community engagement
5. “In the news”

An appendix includes additional information:

1. Newsletters
2. Videos
3. Scrapbook

Steven Weber
Director, Drexel Cybersecurity Institute
1 Acknowledgment

The Drexel Cybersecurity Institute gratefully acknowledges all of the assistance and guidance provided to us by the excellent administrators, faculty, staff, and students at Drexel University. We wish to give particular thanks to the following individuals, listed alphabetically:

Murugan Anandarajan
Norm Balchunas
M. Brian Blake
Debbie Buchwald
Kapil Dandekar
Rob D’Ovidio
David Fenske

Daniel Filler
John Fry
Joseph Hughes
Spiros Mancoridis
Aleister Saunders
Ali Shokoufandeh

We also gratefully acknowledge assistance from the following list of individuals, which is certainly not intended to be in any way exhaustive, also listed alphabetically:

Pramod Abichandani
Susan Aldridge
Marcello Balduccini
LeeAnn Black
Kerry Boland
David Breen
Al Bynum
Sean Clark
Britt Faulstick
Marie Fazio
Lois Gabin-Legato
Caitlin Gauthier
Simon Giszter
Rachel Greenstadt
Allon Guez
Greg Hislop
Tony Hu
Hugh Johnson
Moshe Kam
Nagarajan Kandasamy
Constantine Katsinis
Jennifer Katz

Colleen Kavanaugh
Brian Keech
Sherry Levin
Denise McLeod
Greg Montanaro
Chad Morris
Gaurav Naik
Chika Nwankpa
Alex Olivares
Doug Pfeil
Dionne Queen
Ioannis Savidis
Harish Sethu
James Shackelford
Brenda Sheridan
MaryAnn Skedzielewski
Matthew Stamm
Kimberly Stott
Baris Taskin
Scott White
Kairi Williams
Christopher Yang


2 Research activities

Cybersecurity research today is a far cry from its original focus on network protocols and cryptography. Today’s cybersecurity challenges require an incredibly diverse collection of interdisciplinary approaches, including machine learning, big data, signal processing, algorithm design, computer hardware and software, biometrics, and many others. The scope of research topics pursued by Drexel’s cybersecurity faculty illustrates this diversity. A brief list of topics includes:

1. Cyber crime and online identity theft (Anandarajan and D’Ovidio)
2. Adversarial stylometry (Greenstadt)
3. Sentiment analysis and security informatics (Yang)
4. Network and host anomaly detection (Sethu, Kandasamy, Mancoridis, Weber)
5. Biometric user authentication (Greenstadt and Weber)
6. Media forensics and anti-forensics (Stamm)
7. Wireless jamming and key generation (Dandekar)
8. Hardware security and trust (Savidis, Taskin, Stamm),
9. Malware detection, classification, and mitigation (Mancoridis and Balduccini)

Research activity in these and other areas is broken down into the following categories:

1. Research grants (§2.1)
2. Research articles (§2.2)
3. Graduate student thesis proposals and defenses (§2.3)
4. Research community engagement (§2.4)
5. Technology commercialization (§2.5)

2.1 Research grants

The following is a list of ongoing cybersecurity research grants (initiated prior to 2015):


The following is a list of new cybersecurity research grants (initiated or recommended for funding in 2015):


2.2 Research articles

The following is a list of cybersecurity research articles published in 2015, listed in reverse chronological order:


2.3 Graduate student thesis proposals and defenses

The following is a list of cybersecurity-related M.S. and Ph.D. student candidacy exams, thesis proposals, and thesis defenses, occurring in 2015:


2.4 Research community engagement

The following is a list of engagements with the cybersecurity research community by Drexel faculty in 2015, listed in reverse chronological order:


2.5 Technology commercialization

The following is a list of cybersecurity patents developed by the Drexel research community and marketed by the Drexel Office of Technology Commercialization in 2015:


3 Business development

Drexel University had cybersecurity-oriented business development interactions with the following industry and government entities:

1. Huawei North America Network Division (December, 2015 – present)
2. Bowhead IT Group (November, 2015 – present)
4. FAA ASSURE Center of Excellence in Unmanned Aerial Systems Research (October, 2015 – present)
5. Pro2Serve (September, 2015 – present)
9. U.S. Army CERDEC and ARDEC (persistent relationship)
10. The Judge Group (July, 2015 – present)
11. Areva Nuclear (June, 2015)
12. Exelon/PECO (June, 2015 – present)
13. Turkish Air Force Academy (April, 2015)
16. DSA, Inc. (March, 2015)
17. Northrup Grumman (March, 2015 – present)
18. Comcast (March, 2015 – present)
20. Fitlinxx Inc. (March, 2015)
23. National Security Agency (persistent relationship)
24. Gnostech (February, 2015)
25. L3 Communications (January, 2015 – present)
27. URS/AECOM (December, 2014 – May, 2015)
28. Federal Bureau of Investigation (FBI) (December, 2014 – present)
29. Vanguard (October, 2014 – present)
31. Probaris (October, 2014 – present)
32. Digile (Helsinki, Finland) (September, 2014 – May, 2015)
4 Educational activities

Drexel has established its presence in cybersecurity education through a suite of cybersecurity degrees and certificates. This section breaks down our cybersecurity educational activities into the following categories:

1. courses, degrees, certificates (∂4.1)
2. NSA/DHS CAE-IAE recertification (∂4.2)
3. online cybersecurity education (∂4.3)
5. peace engineering and cybersecurity (∂4.5)
6. corporate cybersecurity education (∂4.6)
7. other educational development activities (∂4.7)

4.1 Courses, degrees, certificates

Academic degree programs and certificates. Drexel cybersecurity-related academic degree programs and certificates include:

1. Masters of Science in Cybersecurity (CYBR)
2. Masters of Science in National Security Management (MSNSM)
3. Bachelor of Science in Computing and Security Technology (CST)
4. Bachelor of Science in Computer Science – Computer Security Concentration.
5. Certificate in Computing and Security Technology
6. Professional Development Certificates in National Security Management, including:
   (a) Cybersecurity, Law & Policy (online)
   (b) Continuity Management (online)
   (c) Homeland Security (online)
7. Undergraduate Minor in Computer Crime

We briefly comment on the CYBR and MSNSM degrees.

Master of Science in Cybersecurity (CYBR):

- The motivation behind this degree program stem from conversations between Drexel University and the National Security Agency about the need for more deeply technical graduate programs in cybersecurity.
- The key novelty of the Drexel cybersecurity degree is its interdisciplinary structure, achieved by integrating coursework from both the Department of Electrical and Computer Engineering (ECE) in the College of Engineering (CoE) and the College of Computing and Informatics (CCI).
- From the degree description, “The program is designed for students with backgrounds in computer engineering, computer science, electrical engineering, telecommunications engineering or other related technical fields and aims to provide deeply technical and specialized training to develop professionals
that are able to understand, adapt, and develop new techniques to confront emerging threats in cybersecurity.”

- Launched as an on-campus program in Fall 2013, and was approved as an online program in Spring 2014.

- Development of the CYBR program was funded by a three-year “capacity building” grant awarded to Drexel in 2012 from the National Science Foundation (NSF) Cyberguards Scholarships for Service (SFS) program (PI: Kapil Dandekar (CoE), Co-I: Steven Weber (CoE), Constantine Katsinis (CCI), and Rachel Greenstadt (CCI)).

- A five-minute video about the degree, featuring remarks by Steven Weber, Constantine Katsinis, and Kapil Dandekar, was produced in June, 2014, and posted to YouTube (see [P] for details).

- An open house for prospective students in the degree program was given on June 2, 2015, with a presentation by Steven Weber, and coordination by Sherry Levin, Chad Morris, and Kapil Dandekar.

**Masters of Science in National Security Management (MSNSM):**

- Offered through the College of Computing and Informatics (CCI).

- From the program page, “The CCI MSNSM involves an understanding of national and homeland security, policy, law, social, and technological environments. As such, modern national security management is an interdisciplinary field built upon the expertise of a wide variety of disciplines. The online MSNSM uses a multidisciplinary approach to targeting advanced topics in security management, emergency management, information technology, risk management, law and policy”.

- Launched as an online program in Fall 2014.

**Cybersecurity-related courses offered.** Drexel offers a solid array of both undergraduate and graduate level cybersecurity courses. We briefly highlight three of these:

- **Web Security I & II (H. Sethu).** A list of topics covered in this two-quarter sequence is given on the left, with the list of subtopics covered in the “symmetric and public key encryption” topic on the right:

  | Security-conscious intro. to web protocols | Symmetric key cryptography; Data Encryption Standard (DES) and the Advanced Encryption Standard (AES); triple DES; cipher block chaining; attacks on cryptographic protocols. |
  | Digital certificates and authentication | Secret key exchange protocols; the Diffie-Hellman Exchange (DHE); attacks on DHE and countermeasures. |
  | A security-conscious intro. to HTML & CSS | Fundamentals of number theory; modular arithmetic; Fermat’s and Euler’s theorems; primality testing; the Chinese Remainder Theorem. |
  | A security-conscious intro. to JavaScript | Principles of public key cryptography; the RSA algorithm and practical implementation details; the choice of public and private keys; strategies for attacking RSA; how secure is RSA? |
  | Origin-based isolation of content | Cryptography in practice on the web; limitations of cryptography. |
  | Encrypted web communications (HTTPS) | |
  | Attacks on Domain Name System (DNS) | |
  | DNS Security Extensions (DNSSEC) | |
  | Security and AJAX | |
  | Web privacy | |
  | Anonymous web browsing | |
  | Illegal hosting and anonymous publishing | |
  | Internet censorship and surveillance | |
  | Elliptic curve cryptography (ECC) | |
  | Web-based malware | |

- **Media Forensics & Security (M. Stamm).** Learning outcomes are on the left, and the list of topics are on the right:

Introduction to image processing Coding & compression Information hiding & digital watermarking Decision theory & machine learning Steganography & steganalysis Multimedia forensics - Manipulation detection Multimedia forensics - Device identification

- Privacy (R. Greenstadt). Learning outcomes are on the left, and the list of topics are on the right:
  Motivation for privacy protection. Measuring privacy using information theory
  Anonymity, unlinkability, unobservability. Data privacy threats and protection measures
  Formalization, modeling, & measurement. Privacy and web mining
  State-of-the-art in privacy technologies. Privacy at the communications layer
  Social media & implications for elec. privacy

The following is a select list of cybersecurity-related course offerings over the past three academic years:

- AY 2015-2016

<table>
<thead>
<tr>
<th>Term</th>
<th>Course</th>
<th>Title</th>
<th>Instructor</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fall 2015</td>
<td>ECEC 457</td>
<td>Security in Computing</td>
<td>L. Trachtenberg</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>INFO 375</td>
<td>Introduction to Information Systems Assurance</td>
<td>C. Mascaro</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>INFO 517</td>
<td>Principles of Cybersecurity</td>
<td>S. White</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>CST 609</td>
<td>National Security Intelligence</td>
<td>S. White</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>HSM 544</td>
<td>Introduction to Homeland Security</td>
<td>S. White</td>
<td>13</td>
</tr>
</tbody>
</table>

- AY 2014-2015
<table>
<thead>
<tr>
<th>Term</th>
<th>Course</th>
<th>Title</th>
<th>Instructor</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CS 303</td>
<td>Algorithmic Number Theory and Cryptography</td>
<td>B. Char</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>CS 475</td>
<td>Computer and Network Security</td>
<td>R. Greenstadt</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>HSM 554</td>
<td>Critical Infrastructure Protection</td>
<td>S. White</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>INFO 333</td>
<td>Introduction to Information Security</td>
<td>C. Carroll</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>INFO 375</td>
<td>Introduction to Information Systems Assurance</td>
<td>C. Mascaro</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>INFO 517</td>
<td>Principles of Cybersecurity</td>
<td>S. White</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>INFO 710</td>
<td>Information Forensics</td>
<td>S. Brown</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>INFO 718</td>
<td>Cybersecurity, Law and Policy</td>
<td>J. Walters</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>ECES 690</td>
<td>ST: Forensic Signal Processing</td>
<td>M. Stamm</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>CST 614</td>
<td>Counterintelligence</td>
<td>S. White</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>HSM 549</td>
<td>Terrorism and Homeland Security</td>
<td>S. White</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>INFO 333</td>
<td>Introduction to Information Security</td>
<td>C. Carroll</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>INFO 712</td>
<td>Information Assurance</td>
<td>P. Grillo</td>
<td>21</td>
</tr>
<tr>
<td>Fall 2014</td>
<td>ECEC 690</td>
<td>ST: Web Security I</td>
<td>H. Sethu</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>CST 609</td>
<td>National Security Intelligence</td>
<td>S. White</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>HSM 544</td>
<td>Introduction to Homeland Security</td>
<td>S. White</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>INFO 333</td>
<td>Introduction to Information Security</td>
<td>C. Carroll</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>INFO 375</td>
<td>Introduction to Information System Assurance</td>
<td>C. Mascaro</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>INFO 517</td>
<td>Principles of Cybersecurity</td>
<td>S. White</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>INFO 710</td>
<td>Information Forensics</td>
<td>S. Brown</td>
<td>19</td>
</tr>
<tr>
<td>AY 2013-2014</td>
<td>ECET 890</td>
<td>ST: SDR Security Laboratory</td>
<td>K. Dandekar</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>CS 303</td>
<td>Algebraic Number Theory and Cryptography</td>
<td>B. Char</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>CS 675</td>
<td>Reverse Software Engineering</td>
<td>G. Naik</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>INFO 333</td>
<td>Introduction to Information Security</td>
<td>C. Carroll</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>INFO 336</td>
<td>Distributed Systems Security</td>
<td>C. Geib</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>INFO 517</td>
<td>Principles of Cybersecurity</td>
<td>S. White</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>INFO 710</td>
<td>Information Forensics</td>
<td>C. McClain</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>INFO 718</td>
<td>Cybersecurity Policy</td>
<td>H. Rishikof</td>
<td>7</td>
</tr>
<tr>
<td>Win 2014</td>
<td>ECEC 690</td>
<td>ST: Web Security II</td>
<td>H. Sethu</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>CS 475</td>
<td>Computer and Network Security</td>
<td>R. Greenstadt</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>INFO 712</td>
<td>Information Assurance</td>
<td>P. Grillo</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>INFO 717</td>
<td>Cyber Crime Law</td>
<td>H. Rishikof</td>
<td>11</td>
</tr>
<tr>
<td>Fall 2013</td>
<td>ECEC 690</td>
<td>ST: Web Security I</td>
<td>H. Sethu</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>CS 680</td>
<td>ST: Privacy in Electronic Society</td>
<td>R. Greenstadt</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>INFO 333</td>
<td>Introduction to Information Security</td>
<td>C. Carroll</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>CJ 276</td>
<td>Introduction to Computer Crime</td>
<td>I Schlanger</td>
<td>23</td>
</tr>
</tbody>
</table>

### 4.2 NSA/DHS CAE-IAE recertification

- Drexel has held the designation as a National Security Agency (NSA) / Department of Homeland Security (DHS) Center of Academic Excellence (CAE) in Information Assurance Education (IAE) for over ten years
• The CAE designation is a credential conferred by the NSA and DHS upon those 2-year and 4-year academic institutions with cybersecurity-related education programs in line with recommended best practices and having the required depth and breadth for its graduates to contribute to the national cybersecurity workforce.

• The DCI has been coordinating the recertification effort for the since May, 2014. Participants include Steven Weber, Kapil Dandekar, Sherry Levin, Chad Morris, Doug Pfeil, Alex Olivares, Constantine Katsinis, and Rich Primerano.

• Recertification requires establishing coverage of each of twenty-two (22) knowledge units (KUs):

| Basic data analysis | Networking concepts |
| Basic scripting | Operating systems concepts |
| Cyber defense | Policy, legal, ethics, compliance |
| Cyber threats | Probability and statistics |
| Databases | Programming |
| Fundamental security design principles | Systems administration |
| IA Fundamentals | Advanced network technology and protocols |
| Intro to cryptography | Database management systems |
| IT system components | Low level programming |
| Network defense | Operating systems theory |
| Network technology and protocols | Security risk analysis |

Each of these KUs has an associated set of topics associated; the topics taught in the various courses must be matched to and cover the various KU topics.

• This designation was critical for Drexel to be named as one of the six universities selected to participate in the USAR P3i program, discussed below.

4.3 Online cybersecurity education

The Drexel Cybersecurity Institute has served as a facilitator between Drexel University Online (DUO), the College of Computing and Informatics (CCI), and the College of Engineering (CoE), regarding marketing of Drexel’s MS in Cybersecurity (CYBR) degree, and to a lesser extent, the MS in National Security Management (MSNSM).

4.4 U.S. Army Reserve Private Public Partnership Initiative (USAR-P3i)

Following the meeting of the Delaware Valley Chapter of the National Defense Infrastructure Association (NDIA) at Drexel on September 9, 2014, Drexel began discussion with LtC. Scott Nelson about the U.S. Army Reserve Private Public Partnership Office initiative (P3i) on cybersecurity education.

The USAR P3i program brings together three key stakeholders for the USAR citizen soldiers: the USAR itself, cybersecurity-related employers, and universities offering cybersecurity-related degree programs. Drexel was identified as one of six initial universities to participate in this program, along with Norwich University, the University of Washington, George Mason University, the University of Texas at San Antonio, and the University of Colorado – Colorado Springs.
As described in the events below, representatives of the six universities attended a ceremony hosted by Lt. Gen. Jeffrey Talley, head of the USAR, in the Raeburn U.S. House of Representatives building in Washington, D.C., on February 10, 2015, wherein a Memorandum of Understanding (MoU) was signed.

A subsequent logistic and planning meeting was held at the University of Colorado – Colorado Springs campus in April, 2015, attended by Drexel representatives Norm Balchunas and Steven Weber. Although the federal funding for this project has been delayed for this fiscal year, Drexel stands ready and willing to work with the USAR on this important program.

Events pertaining to the USAR P3i-Cyber initiative include:


4.5 Peace engineering and cybersecurity

College of Engineering Dean Joe Hughes has initiated partnerships with Bernard Amadei (founder of Engineers without Borders) and the PeaceTechLab (a non-profit organization spun out of the U.S. Institute for Peace in Washington, D.C.), with the goal of establishing Drexel as an academic leader in the field of peace engineering. The Drexel Cybersecurity Institute has been involved in these discussions, and will continue to play an active role moving forward.

4.6 Corporate cybersecurity education

Over the course of numerous cybersecurity-oriented business development meetings over the past several years with Debbie Buchwald and Norm Balchunas, it became apparent that there may be a market for universities to supply tailored cybersecurity education programs to companies. The Drexel Cybersecurity Institute has represented Drexel cybersecurity education infrastructure and capabilities to several major companies over the past several years, including i) Boscov’s and the Merchant Advisory Group (MAG), ii) Comcast, iii) L3 Communications, and iv) Lockheed Martin Corporation Information Systems and Global Solutions (LMCO-ISGS). Towards this end, DCI has been in discussion with both the Drexel Office of Corporate Relations (Debbie Buchwald) and the LeBow College of Business Corporate and Executive Education program (Anna Koulas and Patricia Connolly).

4.7 Other educational development activities

Besides the above initiatives, DCI has also been engaged with several other parties regarding cybersecurity education, including i) the National Cyberwatch Center (Casey O’Brien), ii) the Collegiate Cyber Defense Challenge (Casey O’Brien), iii) the Comcast / UConn. CyberSEED hackathon, iv) the Drexel University Computing Academy (DUCA), v) the Philadelphia Performing Arts String Theory charter school, vi) the Information Systems Audit and Control Association (ISACA) group, vii) the Valley Forge Military College (Wayne, PA), and viii) the National Military Intelligence Association (NMIA).
5 Community engagement

Invited talks given in 2015 by Drexel faculty are listed in §5.1. Events, symposia, invited speakers, and panels organized or co-organized by the Drexel Cybersecurity Institute are listed in §5.2.

5.1 Invited talks by Drexel faculty

Drexel faculty have given the following invited presentations:


5.2 Events organized by the Drexel Cybersecurity Institute

The Drexel Cybersecurity Institute has organized or co-organized the following events in 2015:


Drexel cybersecurity in the news

Drexel cybersecurity-related activities mentioned in the news in 2015 include:


Snapshots of some of these articles are shown on the following pages.

![Image](https://example.com/image1.png)

**Figure 1:** Technical.ly Philly – August 17, 2015.
Why Drexel’s Rachel Greenstadt is a big deal in the privacy technology scene

Greenstadt is working on projects to anonymise developers, sniff out cyber-crime gangs and determine the sensitivity of tweets. She’s also the reason an international privacy technology conference came to Philadelphia this year.

Rachel Greenstadt, a computer science professor at Drexel, runs the school’s Privacy, Security and Automation Lab.
Inside Philadelphia’s growing internet privacy community

Can Philly, birthplace of America, become a hub for Internet freedom, too? A celebrated conference on privacy technology was hosted by Drexel last week.

Drexel University hosted the 2015 Privacy-Enhancing Technologies Symposium (PETS).

Figure 3: Technical.ly Philly – July 8, 2015.
U.S. Army Reserve partners with universities to create cyber security program

FEBRUARY 20, 2015 BY NICOLENA STILES

Every day, the United States is bombarded with new and greater threats to national security — though instead of firearms, these attackers’ weapon of choice is a computer. Finding that the need for cybersoldiers greatly outweighs the supply, the U.S. Army Reserve has partnered with six universities, including Drexel University, to help grow the capabilities of its cyber defense program through the Cyber Public Private Partnership Initiative. Thanks in large part to the work of Nomar Balchunas, a retired Air Force colonel, this past week saw the debut of the program at Drexel.

“With a long history of cybersecurity training and research, really,” Steven Weber, associate professor of electrical and computer engineering, said. “The [National Security Agency] and the [U.S. Department of Homeland Security] have a certification program for universities that meet rather stringent guidelines. If you meet all their guidelines for providing cybersecurity education, then you can be named as a center of academic excellence in information assurance.” Drexel has met those standards for 10 years now, and Weber believes that certification was a major factor for the Army Reserve to consider Drexel as one of its university partners.

Photo Courtesy: Joe Shlabotnik Flickr

Figure 4: Drexel Triangle – February 20, 2015.
Drexel is now one of 6 cybersecurity training centers for the US Army Reserve

The public-private partnership aims to "lessen the skilled soldiers shortage gap," according to the chief of the U.S. Army Reserve.

By Juliana Reyes / REPORTER

Figure 5: Technical.ly Philly – February 11, 2015.
Drexel University has announced a partnership Tuesday with the U.S. Army Reserve (USAR) to offer specialized military cybersecurity training to military personnel.

The university is one of six schools — including the University of Washington, George Mason University, the University of Texas at San Antonio, Norwich University and the University of Colorado-Colorado Springs — to partner with the Army. The U.S. Army Reserve Cyber Public Private Partnership Initiative (Cyber P3I) allows reservists to receive specialized military cybersecurity training as well as enroll at Drexel using scholarships provided through the program and the GI Bill.
A  Newsletters

The Drexel Cybersecurity Institute publishes a “near-monthly” newsletter:

December, 2015
November, 2015
October, 2015
September, 2015
June, 2015
May, 2015
April, 2015
March, 2015
February, 2015
January, 2015

The newsletters have been developed by Norm Balchunas, Dionne Queen, Brenda Sheridan, and Kerry Boland. The newsletters are shown on the following pages.
December 2015 Newsletter

In this issue:
- Anonymous Declares War on ISIS
- White House Launches Cybersecurity Practices
- White House Reports on Big Data Discrimination
- Experts Sound Off on Why Companies Are Still Being Hacked
- Spotlight Profile
- Seeking Cyber Students
- Minors in Computer Science/Information Tech
- Cyber Risk Alerts/Training

SPOTLIGHT

Professor Nago Kandassamy

An Andrew ER Professor of Electrical and Computer Engineering

Professor Kandassamy is an Associate Professor in the Department of Electrical and Computer Engineering. He teaches and conducts research in the areas of computer engineering, with a focus on computer networking and distributed systems. His current research interests include the design and analysis of distributed systems, computer architectures, and testing and validation methodologies. Professor Kandassamy received his PhD from the University of Illinois at Urbana-Champaign and his MS and BS from the Indian Institute of Technology, Madras.

Contact Info
Office: 2052 NS
Phone: 215-951-1795
Email: kandassamy@seas.drexel.edu

Cybersecurity Institute

Cybersecurity Institute

Cybersecurity Institute

Cybersecurity Institute

Cybersecurity Institute

Cybersecurity Institute

MINORITIES IN COMPUTER SCIENCE/INFORMATION TECH

Latinas Leaders Pushing for More Minorities to Fill Future Computer Science Positions

Virginia-based nonprofit advocacy agency The National Heritage Foundation is urging minority students to pursue computer science, in light of the U.S. labor gap. The Founding Chair and President of The National Heritage Foundation, Philip Corso, also launched a new campaign called The Code is a Second Language. The campaign focuses on the importance of computer programming and coding among minority communities. President (PDC) of The Hispanic Heritage Foundation, shown speaking at an event, has spoken about how minorities have been historically left out of the tech industry. This campaign aims to address the issue of diversity in the tech industry and encourage minority students to pursue computer science.

Read more on techcrunch.com

Click to view the top 10 most influential Latinos in tech

SPOTLIGHT

Anonymous Vows to Take Down ISIS with Cyber Tools

International "indictment" network Anonymous has released a video statement declaring war on ISIS, a terrorist group that started more than 10 years ago in Syria. ISIS has claimed three consecutive cyber attacks, with the latest being on the Syrian Civil War, and the third on the ISIS’s official website. The group’s statement was released following a recent attack, French President Francois Hollande called these actions "on war with the world in territories that have not yet been conquered by ISIS.

- Video Statement from Anonymous - YouTube Video: 1:38 in length (in English with English subtitles)
- BBC News Video: 54. Anonymous vs. ISIS
- BBC News: Anonymous has taken out 6 from ISIS’s websites
- Speak to Drexel's IT director to learn more about joining the fight!

White House Reports on How Companies "Big Data" Can Be Used to Discriminate

The White House is calling for federal officials to develop a set of cybersecurity methods in dealing with cyber hacking and is now looking to integrate these practices. The review is currently being conducted in light of the White House’s new initiative in cybersecurity and privacy protection, which focuses on the cyber threat to national security and economic challenges. The review is expected to lead to the development of a national plan that can be used to protect the U.S. economy from cyber attacks.

- Read more on fortune.com
- The White House Summit on Cybersecurity and Consumer Protection on Feb. 19, 2015 at Stanford University

Big Data Discrimination (Video 8:28)

White House Councillor John Podesta and WHBCN Host Alexie Glade discuss the need for regulations on consumer-collected Big data, the value of consumer privacy and the possible discrimination that can result from the use of consumer data. Guest speakers include: Mona Chalabi, Winning, women's rights, and the role of the internet in different societies. Experts sound off on why companies are still being hacked

Cybersecurity experts state that the reason as many companies are being hacked is because they are using old methods of protecting their infrastructure. With the increased use of advanced technology, and with employees using their personal devices such as tablets, smartphones and laptops, hackers are able to gain access to company’s critical data and information. Some cybersecurity experts believe that implementing a multi-layered approach focuses on a methodology that offers protection for both the network and data, which will result in protection from both outsider and insider threats.

Read more on cbc.com
Spotlight: Matthew C. Stann, Assistant Professor

Matthew C. Stann is an Assistant Professor in the Department of Computer Science at Drexel University. His research focuses on computer security and privacy, with a particular interest in understanding how people interact with security and privacy features in technology.

CYBER RISK ALERTS AND TECH NEWS


Microsoft Invests $75 Million in Schools to Advance Computer Science

Microsoft has announced a $75 million investment in schools to advance computer science education. The initiative aims to support the development of computer science programs and teacher training in high schools across the United States. This investment is part of Microsoft’s broader commitment to expanding access to computer science education.

China Invests $1.57 Billion in Cloud Computing

China has announced an investment of $1.57 billion in cloud computing companies. The funds will support the development of cloud computing infrastructure and services. The investment is expected to accelerate the growth of the cloud computing industry in China, driving innovation and supporting economic development.

Pentagon Collaborates with Silicon Valley Technology Firms to Aid Wounded Troops and the Military

The Defense Advanced Research Projects Agency (DARPA) has announced a new initiative to collaborate with technology firms in Silicon Valley to develop innovative technologies for the military. The initiative aims to accelerate the development and deployment of cutting-edge technologies to support the needs of the military.

Silicon Valley Addresses Diversity by Targeting Black Students

Tech companies in Silicon Valley are focusing on diversity initiatives to target Black students. These efforts include scholarships, mentorship programs, and partnerships with historically Black colleges and universities. The initiatives are designed to increase diversity and promote inclusive growth in the technology sector.

Dealing With Privacy Threats and Data Breaches

As data breaches become more frequent, businesses and individuals are increasingly concerned about protecting their personal information. Best practices for dealing with privacy threats include regular security updates, strong password management, and staying informed about the latest security threats.

Another Russian Hack

Russian hackers continue to be a threat to global cybersecurity. Recent attacks have targeted various sectors, including government agencies, financial institutions, and critical infrastructure. The Russian government has denied any involvement, but evidence suggests otherwise.

Video: 2013 Cybersecurity Defense Protection

This video provides insights into cybersecurity defense strategies and practices. It covers topics such as threat monitoring, incident response, and the importance of continuous improvement in cybersecurity measures.

Video: Is the Brain Faster Than Any Super Computer?

This video explores the capabilities of the human brain compared to super computers. It discusses the brain’s ability to process information and its potential for further development in the field of artificial intelligence.

World’s Fastest Computer Up and Running

The world’s fastest computer, called "Elastic Cloud," has been successfully deployed. This supercomputer is designed to handle massive data processing and complex computational tasks, setting a new benchmark for computational power.
Spotlight:
Ioannis Savvidis

Ioannis Savvidis is an Assistant Professor at Drexel University, where he is Director of the Integrated Circuits and Electronic (ICE) Design and Analysis Laboratory in the Department of Electrical and Computer Engineering. He received his B.S. in electrical and computer engineering and some additional electrical engineering from Drexel University, Drexel, PA, in 2005. He also received both his M.S. and Ph.D. degrees in electrical and computer engineering from the University of Rochester, Rochester, NY, under the guidance of Professor Elad Tur and Erikih. As part of his doctoral work, he developed circuit design techniques and algorithms for the design of reconfigurable and heterogeneous three-dimensional integrated circuits. He is the new editor-in-chief of VLSI Design and has been selected for the 2015 IEEE Presidential Young Engineer Award.

Contact Info
Office: Snitzer 106
Phone: 215-764-8000
Email: savvidis@ecn.drexel.edu

Privacy Enhancing Technologies Symposium
(PETS) Philadelphia, PA

The annual Privacy Enhancing Technologies Symposium (PETS) brings together privacy researchers and practitioners from around the world to discuss recent advances and new perspectives. PETS addresses the design and evaluation of privacy services for the Internet and other data systems and information networks.

PETS Website

Seeking Cyber Students:
Drexel Women in Computing Society (WCS)

“Our purpose is to support, network, and help in pursuing a degree in the broad field of computer science. WCS will enhance communication among members who are pursuing a degree in computer science through informal dinners and gatherings, social events, webinars, and advocacy for computer science and its members as needed. The ultimate goal is to empower women in computer fields to succeed and thrive in the Drexel community and beyond.”

Click to join Drexel Women in Computing Society (WCS)

The Master of Science (MS) Degree in Cybersecurity at Drexel’s College of Engineering

The Master of Science (MS) in Cybersecurity is an interdisciplinary program that prepares students with both the theoretical background and practical experience necessary to become leaders in the ever-changing technical landscape of cybersecurity. This program is designed for students with backgrounds in computer engineering, computer science, electrical and electronic engineering, or other related technical fields.

Two New Bug Threats for MAC Computers

Two new bugs are currently affecting Macintosh computers. The first is a bug that produces incorrect random numbers and the second is a threat of total permanent control of your Mac through a hacker. This first malware is called `Utterase’ and appears to be the first to successfully allow attackers to steal secrets from the reader and gain control over your computer. The second malware is called `Phantom’ and allows attackers to steal secrets from your computer and access your computer’s secrets.

CYBERSECURITY DEFENSE/PROTECTION:

Homeland Security NewsWire

Department of Defense (DoD) Cybersecurity

The Future of Cooling is in Girl Power

Girls Who Code is a nonprofit group that is looking to increase the number of women in technology. They reported that in 2014, 37% of computer science graduates were women. However, the number has dropped to just 18% of women today. In response, Girls Who Code recently created a seven-week camp called Girls Who Code Summer Immersion Program, which actively pursues and encourages high school girls to attend to fill the growing gap.

Drexel’s CCI Faculty Win in on Pope Francis’ Visit to Philadelphia

Drexel Senior University College of Computing & Informational Sciences recently posted several news stories on the upcoming visit of Pope Francis at the World Meeting of Families in Philadelphia. In September 2015:

Jennifer Borker, PhD, was quoted in a July 24 Philadelphia Inquirer story about problems with SEPTA’s website during the sale of special train passes.

Scott White, PhD spoke with ABC10 on Aug 9, about the City of Philadelphia’s plans to shut down major roadways. White was quoted in a July 9, Philadelphia Inquirer story on the successful use of traffic from the City of Philadelphia and law enforcement. He was also interviewed on WURD Radio (965 AM) on Aug. 11 about security measures for the City is taking during the Pope’s visit.

Ko Haro’s Ph.D. thesis on the technological challenges in estimating the crowd size and his research in computer vision detection of unusual events in crowds.

Meet HERMES, A Bipedal Robot with Human Reflexes Created at MIT

HERMES, called a “human-machine interface that keeps balance, with human reflexes,” was developed by MIT students to one day be released and to help aid in disaster areas. These types of robots would explore disaster zones controlled by human operation via a remote, safe location.

Read more on MIT News
Upcoming Events:

Drexel University Cybersecurity Institute Symposium Speaker Presentation with David Whipple
Innovating Security!

Date: June 24, 2015
Location: 4041 Market Street, 3rd Floor, Cybersecurity Lab, Room 226
Time: 12:00 PM - 1:30 PM

Abstract: This presentation will discuss information Security principles as they relate to organizational culture and the trend of innovation. Recent research points to the lack of compliance between Security and Innovative cultures as a key reason for security breaches. Case Studies will be presented that strengthen security within innovative organizations. There are five main traits that organizations can implement that can strengthen security within innovative cultures. How is your business or your doing?

Speaker: David Whipple, Whipple is the Principal Security Architect for Exelon Energy with his base at PG&E in Philadelphia.

David Whipple Bio
Click RSVP! Link to register

This Event will be recorded and will be available on CStv's Pay-By-View Channel

Contact Information
Name: Norm Ehrlichman
Phone: 215-571-3445
Email: nbe@reed.edu

4A Security and Duane Morris presents: Cybercrime: Preparing Leadership for a Breach

Homeland Security: Gov't Data Breach of OPM and Interior Dept.

The Department of Homeland Security (DHS), the Department of the Treasury, and the Department of the Interior have all suffered a data breach. The bureaucratic bungle of the federal employee personnel data records. The compromised data was stolen from the Office of Personnel Management (OPM) and the Interior Department. Chinese hackers are suspected to be behind this recent breach. Security experts states that this action is inexcusable and better use of data technologies such as encryption could have increased security and preventing theft of this data would have been avoidable. The following YouTube video reports that the damage is much worse than what was reported earlier. YouTube reports that the 14 million government employees that were affected by the Interior, the Department of National Security, the Pentagon, FISA and OPM personnel. The compromised personal records consisted of intelligence data, security clearances, social security numbers, birthdays, and home addresses.

Read more on Fox News
YouTube Video 1:09

CIA Chief Believes Gov’t Data Breach Can Entice China to Recruit U.S. Officials as Spies

WSJ Video 1:07 - NSA/CIA Director Michael Hayden discusses how China can possibly recruit U.S. officials as spies as a result of the millions of recently stolen Government personal records

NPR Discussion: How Government was Breached

The below audio link is correspondence between Audie Cornish, co-host of NPR's All Things Considered and Dina Temple-Raston, Immigration correspondent at NPR. They discuss the various matter of exactly how private information of millions of people are compromised and stolen from US Government.

Click link to listen to audio 3:57

NPR (National Public Radio) is a mission-driven, multimedia news organization and media program producer. NPR is also the leading membership and representation organization for public radio.

In The Hot Seat: OPM Director Katherine Archuleta and China Hack

YouTube Video 3:26 - OPM Director Katherine Archuleta is questioned heavily by Federal Agency in regards to OPM data breach of U.S. personal records and the 'negligent' security system that was used.

Hacking of LastPass

LastPass is one of many password manager tools considered controversial in the security community. Those in favor of password managers appreciate the ease and simplicity of setting up different passwords for various accounts without having to remember them all. On the downside, there is the risk of the password manager being breached and hackers gaining access to all the managed accounts. Joe Stewart, the LastPass chief executive, announced this past Monday through his blog, that last Friday, LastPass network was breached. Hackers were able to obtain user email addresses, password reminders and encrypted master passwords.

Read more on NYTimes blog

NetDiligence is a Cyber Risk Assessment and Data Breach Services company.

Since 2001, NetDiligence have conducted thousands of enterprises-level cyber risk assessments for a broad variety of corporate clients, including well-known names in banking, brokerage, mortgage, insurance, clearinghouses, and other financial service sectors. They have also assessed major internet-based retailers, online auctions, B2B service providers, software companies, medical providers, universities, and a significant percentage of the Fortune 2000.


Seeking Cyber Students for: Master of Science (MS) Degree in Cybersecurity at Drexel University's College of Engineering

Click link to see course curriculum, requirements and graduate school program specificities.

Click link to Drexel University Cybersecurity Institute’s Website and Contact Info
May 22, 2015 - In This Issue:

Penn State’s Engineering College Computer Network Hacked by Chinese Hackers

High Demand to Hire Cybersecurity Professionals by Government

Russia and China Create Their Own “New World Order”

Upcoming Events

Spotlight: Drexel’s Ph.D Students

Upcoming Events:

Drexel University
College of Engineering
M.S. in Cybersecurity Information Session

Please join us for an information session to learn about the Master of Science in Cybersecurity degree program offered at Drexel University’s College of Engineering (CoE).

Date: Tuesday, June 2, 2015
Registration: 4:45 PM - 5:15 PM
Session: 5:15 PM - 7:30 PM
Location: Boscone Research Enterprise Center, Philadelphia, PA

CYBERSECURITY NEWS:

Penn State’s Engineering College Computer Network Hacked by Chinese Hackers

Last Friday, it had been discovered that for over two years, Chinese hackers have been probing through the computer network of Penn State’s College of Engineering. The university recently has been developing sensitive technology for the U.S. Navy. As a safety precaution, the engineering college’s computer network has been taken down for several days. The unexpected breach leads authorities to believe that foreign spies are using universities as a gateway to obtain personal, discreet information about U.S. commercial and defense secrets.

RSPV: To register for this event and for a complete list of College of Engineering master’s and doctoral programs, please click here: [Registration and Event Details]

Click link to learn more about:

Master of Science in Cybersecurity degree program

For additional information, please contact Sherry Levin at 215.571.3661, or visit: Drexel.edu/eng/policy

Innovating Securely!

Date: 24 June
Time: 12:00 noon
Location: TBD

Abstract: This presentation will discuss information security principles as they relate to organizational culture traits, focusing on the trait of innovation. Recent research points to the lack of relationship between Security and Innovative culture as a key reason for security breaches. Case Studies will be presented that strengthen security within innovative organizations. There are five main traits that organizations can implement that can strengthen security within innovative cultures. How is your business or you doing?

Speaker: David Whipple. Whipple is the Principal Security Architect for Exelon Energy with his home base at PECO in Philadelphia.

David Whipple Bio[pdf]

Spotlight:

Drexel’s Ph.D Student Profile

Bradford D. Boyle
Ph.D Candidate

Bradford D. Boyle is currently a Ph.D candidate in the Modeling and Analysis of Network Labs at Drexel University, advised by Steven Weber.

Boyle’s research interests include: distributed source coding, combinatorial optimization, multiterminal information theory, and wireless networking.

Read more about Bradford’s Research at Drexel in His Own Words [pdf]

Email:
bradford.d.boyle@drexel.edu

Personal website:
hp://www.bradfordboyle.com

Office: Boscone 604

High Demand to Hire Cybersecurity Professionals by Government

Every week in the news, it is reported about the damaging effects of cyber hackers. With cyber hacking comes financial loss, loss of information, decreased privacy and damaged reputations. Why a person would hack in the first place varies, it could be either for the challenge, to obtain information, to seek fame or for sharpening and honing programming skills. Either way, it causes damages to computing devices of individuals and/or businesses which may result in millions of dollars lost. To combat this growing epidemic, government agencies and the U.S. military are stepping in and are currently seeking the best cyber professionals to address the issue of cyber hacking.

Read more on Homeland Security News Wire

Russia and China Create Their Own “New World Order”

China’s President Xi Jinping and Russia’s President Vladimir Putin make no secret of their strong alliance with each other. Their bond was made stronger recently by signing dozens of bilateral agreements including one that included the shared agenda of promising not to “hack” one another’s country. James Lewis, a cybersecurity researcher at the Center for Strategic and International Studies, believes that this is just another display of Russia’s and China’s disdain for America. Lewis states that this latest move is the two countries’ way to “undermine American dominance of the tech industry and the Internet.”

Read more on US News

NetDiligence® is a Cyber Risk Assessment and Data Breach Services company. Since 2001, we have conducted thousands of enterprise-level cyber risk assessments for a broad variety of corporate clients, including well-known names in banking, brokerage, mortgage, insurance, clean-house, and other financial services sectors.

Cyber Risk News Alert, Vol 159 - May 19, 2015

STEALTH

Unisys Stealth is a global information technology company that solves complex IT challenges at the intersection of modern and mission critical. We work with many of the world’s largest companies and government organizations to secure and keep their mission critical operations running at peak performance.

Unisys Stealth

The Computing Research Association (CRA) is an association of more than 200 North American academic departments of computer science, computer engineering, and related fields; laboratories and centers in industry, government, and academia engaging in basic computing research, and affiliated professional societies.

Computing Research News
Sources Claims Attack on White House Unclassified System by Russia

As late as last October, the White House noticed suspicious activities on its unclassified network. Sources claim hackers working for the Russian government was able to breach the White House unclassified system and was able to receive sensitive information including the president's non-public email parts in real-time. Even though the unclassified system is not a high priority as the classified system, this information is still considered valuable to foreign spys.

Click link to read full article and see video

Overcoming Shame to Address Cyberbullying

Speaking bravely about her now infamous scandal with then President Bill Clinton that came out to the public through social media in 1998, Monica Lewinsky courageously speaks about this painful experience. Admitting her past mistakes, addressing cyber bullying and public shaming through social media, Monica Lewinsky today is a more confident and stronger woman because of it.

Click link to read and view video of Monica's Story
**UPCOMING EVENTS**

**AI Drexel Cybersecurity Institute Symposium:**

Data Privacy Technology Challenges in 2015

Navigant Consulting, Inc. and the AI Drexel Cybersecurity Institute Symposium invite you to attend a complimentary 1 hour presentation on Data Privacy Technology Challenges in 2015. We will focus on:

- New Technologies and Data Privacy Challenges
  - Google Glass, Glafox, Smartphones with Camera and Recording capabilities, Smartwatches, Fitbit
- Existing Technologies
  - Social media prevalence (Facebook, Twitter, Instagram)
  - BYOD acceptance, the "connected" workforce and their mobile device expectations
  - Please send the X-rays of my iPad and I will check them once I got home.
- New and existing risks
  - Dropbox, Snapchat, Yik Yak
- Gamification
- How do you assess the risk of something without knowing its existence?

Speakers will be Darin Beiley and Stephen Ramsey of Navigant

Date: March 26, 2015
Location: Rush Building, Room 014, 30 N. 33rd Street, Philadelphia, PA
Time: 12:00 to 1:00pm
Lunch provided by Navigant

Register:
https://sites.col.drexel.edu/navy/cybersecurity-institute-symposium-3-26-15/

**NATIONAL CYBERSECURITY INSTITUTE SYMPOSIUM:**

Distinguished Speaker Presentation - Dr. Hal Berghel

The Future of Digital Money Laundering

This talk investigates several types of digital money laundering, characterised by sources (failed states, state-aware, leptocratic states, terrorists, extremists, and individuals), means (credit- and debit-card exploits, international funds transfers, klepto banks, "gift-card" exploits), and purpose (terrorism, narco-trafficking, "electronic crime, internet fraud"). These categories are introduced by their identifying events-of-interest. Implications on shadow economies, degrees of sophistication, and case studies are discussed. Each crime will be explicitly linked geographically and politically to sources, and may include discussion of actual cases. Several micro- and macro-level mitigation strategies will be discussed.

Date: March 31, 2015
Location: Paul Peir Alumni Center, 3142 Market Street, Philadelphia, PA
Time: 12:00 to 1:00pm

Register:
https://sites.col.drexel.edu/navy/cybersecurity-institute-symposium-3-31-15/

**STAY CONNECTED WITH CURRENT EVENTS**

http://drexel.edu/visit/about/press-room/events/

---

**CYBERSECURITY SNIPETS:**

**Government Accounting Office identified weaknesses in our National Airspace Systems to cyber-based threats**

While the Federal Aviation Administration (FAA) has taken steps to protect its air traffic control systems from cyber-based and other threats, significant security control weaknesses remain, threatening the agency’s ability to ensure the safe and uninterrupted operation of the national airspace system (NAS). These include weaknesses in controls intended to prevent, limit, and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on FAA’s systems. Additionally, shortcomings in boundary protection controls between two secure systems and the operational NAS environment increase the risk from these weaknesses.


**PENDING PROPOSALS**

**Cyber-Physical Systems (CPS)**

Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability that will far exceed the simple embedded systems of today. CPS technology will transform the way people interact with engineered systems – just as the Internet has transformed the way people interact with information. New smart CPS will drive innovation and competition in sectors such as agriculture, energy, transportation, building design and automation, healthcare, and manufacturing.

View more: http://www.nsf.gov/funding/pgm_summ.jsp?pgm_id=503286

**Secure and Trustworthy Cybersecurity (SaTC)**

Cyberspace has transformed the daily lives of people for the better. The rush to adopt cyberspace, however, has exposed its fragility and vulnerabilities. Corporations, agencies, national infrastructure and individuals have been victims of cyber-attacks. In December 2011, the National Science and Technology Council (NSTC) with the cooperation of NSF issued a broad, coordinated policy framework for cybersecurity research and development to “change the game,” minimize the misuse of cyber technology, bolster education and training in cybersecurity, establish a science of cybersecurity, and transition promising cybersecurity research into practice. This challenge requires a dedicated approach to research, development, and education that leverages the disciplines of mathematics and statistics, the social sciences, and engineering together with the computing, communications and information sciences.

View more: http://www.nsf.gov/funding/pgm_summ.jsp?pgm_id=504799

**Cybersecurity Innovation for Cyberinfrastructure (CICI)**

Advancements in data-driven scientific research depend on trustworthy and reliable cyberinfrastructure. Researchers rely on a variety of networked technologies and software tools to achieve their scientific goals. These may include local or remote instruments, wireless sensors, software programs, operating systems, database servers, high-performance computing, large-scale storage arrays, and other critical infrastructure connected by high-speed networking. This complex, distributed, interconnected global cyberinfrastructure ecosystem presents unique cybersecurity challenges. NSF-funded scientific instruments are specialized, highly visible assets that present attractive targets for both unintentional errors and malicious activity; untrustworthy software or a loss of integrity of the data collected by a scientific instrument may mean corrupt, skewed or incomplete results. Furthermore, often data-driven research, e.g., in the medical field or in the social sciences, requires access to private information, and exposure of such data may cause financial, reputational and/or other damage.


**Dr. Steven Weber**
Founding Director,
AI Drexel Cybersecurity Institute
steveb@coxe.drexel.edu

**Norm Balchunas, Col., USAF (Ret.)**
Operations Director,
AI Drexel Cybersecurity Institute
nbal@coxe.drexel.edu

http://coxe.drexel.edu/cybersecurity

*If you wish to unsubscribe from this newsletter, please reply directly to the email.*
Cybersecurity Snippets

We Are On Notice: Terrorists Target Grids
Brattle, 27 Jan 15, Frank Cuffe

On Sunday, jihadists attacked a main power line in Pakistan's Balochistan’s Naseerabad district. As a result, 160 million Pakistanis were left in the dark and two nuclear power plants were knocked off line.

View full article: http://pro.aol/jyynfIl

Cybersecurity Now Key Requirement For All Weapons: DoD Cyber Chief

Cybersecurity - it's not just for networks anymore. The trend towards what's called "the Internet of Things" means targets can be anywhere.

View full articles: http://pro.aol/K6xQ486

Army Drone's Electronic-Attack Vulnerability Worries Weapons Testers
Inside the Army, 23 Jan 15, Ellen Mitchell

The Army’s “Shadow” unmanned aircraft system may be vulnerable to cyberattacks, according to the latest annual report by the Pentagon’s director for operational test and evaluation. Though the RQ-1B Shadow is “survivable in the presence of older, less capable electronic warfare threats,” further testing is required to determine the aircraft’s performance in the presence of more advanced weaponry.

The report added that cybersecurity testing - which took place in May 2015 at Ft. Bliss, TX, and White Sands Missile Range, NM - demonstrated that the aircraft “has exploitable vulnerabilities that could impact its operations.” Gilmore notes that testing did not address Detect, Reject, or Restore capabilities of the unit equipped with the Shadow system, “nor did it test the cybersecurity of the aircraft’s Universal Ground Control Station.”

Drexel partners with U.S. Army on cybersecurity

Drexel University has announced a partnership with the U.S. Army Reserve (USAR) to offer specialized military cybersecurity training to military personnel.

The university is one of six schools - including the University of Washington, George Mason University, the University of Texas at San Antonio, Norwich University and the University of Colorado-Colorado Springs - to partner with the Army. The U.S. Army Reserve Cyber Public Private Partnership Initiative (Cyber P3) provides opportunities for universities to receive specialized military cybersecurity training as well as enroll at Drexel using scholarships provided through the program and the GI Bill.

View full article: http://www.phillyvoice.com/drexel-partners-us-army-cybersecurity-program/

Dr. Steven Weber and Dean David Fenske along with partner universities celebrate the signing of the USAR FISI Cybersecurity certificate.

Follow us on Twitter View our profile on LinkedIn

Dr. Steven Weber
Founding Director, Drexel University Cybersecurity Institute sweber@coe.drexel.edu

Norm Belchunes, Col., USAF (Ret.)
Operations Director, Drexel University Cybersecurity Institute nbelchunes@drexel.edu

http://coe.drexel.edu/cybersecurity

*If you wish to unsubscribe from this newsletter, please reply directly to the email.
**Ad Drexel Cybersecurity Institute Symposia**

Healthcare data protection, mobile applications and HIPAA-HITECH, presented by Ben Goodman.

A comprehensive look at organizational and technical challenges to secure privacy of protected health information in the fast evolving world of smartphone enabled health care applications.

Speakers will represent the technical, legal, policy and risk management perspectives.

**Date:** February 25, 2015  
**Time:** 12.00PM  
**Location:** 3401 Market Street, Suite 300

---

**Scholarship For Service (SFS)**

Scholarship For Service (SFS) is a unique program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government’s critical information infrastructure. This program provides scholarships that may fully fund the typical costs incurred by full-time students while attending a participating institution, including tuition and education and related fees. Additionally, participants receive stipends of up to $20,000 for undergraduate students, $25,000 for master’s degree students and $30,000 per year for doctoral students. The scholarships are funded through grants awarded by the National Science Foundation.

---

**2014 Cyber Attacks Statistics**

The following is attached as a macro-indicators of the threat landscape and the corresponding trends.

---

To view more statistics of the 2014 Cyber Attacks, please visit the link below.

B Videos

The Drexel Cybersecurity Institute has developed a strong online video presence, including tapings of the DCI Symposia listed below. These videos are available at the Drexel College of Computing and Informatics (CCI) YouTube channel cybersecurity “playlist”, accessible here:

https://www.youtube.com/playlist?list=PLZvvnkvrLLmQ1-hoxgp8X3OlkNp14wyTc

1. June 24, 2015: Innovating securely
Summary: This presentation will discuss Information Security principles as they relate to organizational culture traits, focusing on the trait of innovation. Recent research points to the lack of relationship between Security and Innovative cultures as a key reason for security breaches. Case Studies will be presented that strengthen security within innovative organizations. There are five main traits that organizations can implement that can strengthen security within innovative cultures. How is your business or you doing?

Figure 7: Invited lecture: “Innovating securely” by David Whipple (Exelon).
Video title: Public and private cloud network security: mitigating virtual machine vulnerabilities
Event date: May 13, 2015
Video published: May 19, 2015
People: Rob Johnson, Unisys
URL: https://www.youtube.com/watch?v=RzZx7axEMHk
Summary: VM security is a major issue for both public and private cloud deployments. Virtual Machines may have particular risks regarding data at rest and in motion, and the credentials and certificates that protect them. The risks to VMs increase as IT’s control over their compute environments decreases. This talk highlights some of those risk factors and presents an approach to mitigate them.

Figure 8: Invited lecture: “Public and private cloud network security: mitigating virtual machine vulnerabilities” by Rob Johnson (Unisys).
Video title: Life threatening hacks: mobile health and medical device data security
Event date: February 25, 2015
Video published: March 2, 2015
People: Ben Goodman (moderator), Lisa Clark and Angel Rivera (panelists)
URL: https://www.youtube.com/watch?v=Q-9nk2a3hYs

Figure 9: Symposium: “Life threatening hacks: mobile health and medical device data security” with moderator Ben Goodman (President, 4A Security) and panelists Lisa Clark (Partner, Duane Morris, LLP) and Angel Rivera (Developer, Point.io).
C Scrapbook of events and meetings

The following pages hold pictures, announcements, and agendas for important events.

Memorandum of Understanding for National CyberWatch Center Members

This document will serve as an agreement between Drexel University and the National CyberWatch Center, headquartered at Prince George’s Community College.

Mission/Objectives: The National CyberWatch Center is a consortium of higher education institutions, public and private schools, businesses, and government agencies focused on building and maintaining a stronger information assurance workforce. Members are critical to the growth and strength of the consortium. Members provide advice, support, and leadership for National CyberWatch Center programs and activities, and advocate National CyberWatch Center programs to the broader community.

By signing, you affirm that you have read the attached document outlining Member Benefits and Responsibilities, have a clear understanding of the expectations for your institution and for the National CyberWatch Center, and agree to become an active member of the Consortium.

____________________  November 11, 2015

Institution Representative (Signature)  Date

Institution Representative (Print): Steven Weber

Email: sweber@coe.drexel.edu

Title: Director of Drexel Cybersecurity Institute

Professor in Department of Electrical and Computer Engineering

Name of Institution: Drexel University

Mailing Address: 3141 Chestnut St., Philadelphia PA, 19104

Phone: (215) 895-0254

____________________  __________________________

Casey O’Brien, National CyberWatch Center Director  Date

Please email completed form to tkepner@cyberwatchcenter.org or fax to 1-707-307-0266.

Figure 10: November 11, 2015 – Memorandum of Understanding between Drexel University and the National Cyberwatch Center.
Program Leaders

Ben Goodman

Lisa Clark

Duane Morris

Conference Mission

“Health and medical regulators are promising audits and tougher enforcement while law enforcement warns that health data is under attack. Meanwhile, there is no shortage of ‘solutions’ promising to protect data and prevent breaches, but not enough resources or even time in the day to review all the options. Of course, cyber security is not just an IT problem. It is a risk management problem that requires an interdisciplinary team approach. And that’s what inspired the mission for this event.” – Ben Goodman, 4A Security & Compliance

Figure 11: October 22, 2015 – Flier for the 4A Healthcare Data Security and Privacy Symposium, held at the Gerri C. LeBow building.
Figure 12: April 20, 2015 – Agenda for the Army Reserve Cyber Private Public Partnership Design Workshop, held on the campus of the University of Colorado in Colorado Springs.
MEMORANDUM OF UNDERSTANDING
Between
Drexel University
And
The United States Army Reserve

This Memorandum of Understanding ("MOU") is between The United States Army Reserve (hereinafter referred to as "USAR") and Drexel University (hereinafter referred to as "Drexel"), and will be effective upon the signature of both parties ("Effective Date"). USAR and Drexel are both referred to in the alternative as a "Party" and collectively as the "Parties".

Whereas USAR and Drexel wish to enable cooperation and exchange in academic areas of mutual interest;

Now, therefore, USAR and Drexel, as Parties to this MOU, set forth the following:

I. BACKGROUND

Parties will collaborate to develop a cyber-education program. The cyber course offerings will map to the National Security Agency ("NSA") and Department of Homeland Security ("DHS") Knowledge, Skills, and Abilities ("KSA’s") pathways to achieve depth and breadth of cyber security education that align with USAR’s need for developing the managerial and journeyman skill sets necessary to defend and secure the Nation’s critical cyber-based systems.

II. AUTHORITIES

This MOU is entered under the provision and in support of the following statutes and Executive Orders:

A. Veterans Employment Opportunities act of 1998 (PL105-339)

B. Title 38, Veterans’ Benefits, Chapter 42 Employment and Training of Veterans (38 U.S.C. 4211, et seq)

C. The Uniformed Services Employment and Reemployment Act of 1994 (PL 103-353)

D. Title 38, Employment and Reemployment Rights of Members of the Uniformed Services (38 U.S.C. 4301-4335)

III. PURPOSE OF THE MOU

The purpose of this MOU is to record the mutual understanding and cooperative spirit with which the Parties named in this MOU intend to work together to offer additional academic course and degree offerings which complement each other and experiential learning to support USAR’s plan for educational advancement among its personnel.

IV. TERMS OF UNDERSTANDING

Figure 13: April 20, 2015 – First page of the final signed Memorandum of Understanding between the U.S. Army Reserve and Drexel University.
BALANCING ACT
Big Data, Cybersecurity and Privacy

Please join us for a symposium that will bring together perspectives from technologists, industry leaders and other stakeholders to develop a view of the building convergence of big data and cybersecurity and the challenges to privacy. Specifically, our goal is to improve understanding of privacy concerns against a backdrop of increasing data apertures and the exponential amount of vulnerable data. CVDI has focused on how big data technologies are transforming the way we do business. The challenge now is how that data is secured and privacy is protected in the new big data ecosystem.

Confirmed speakers include:

- **Keith Morales**
  Assistant Vice President & Information Security Officer, Federal Reserve Bank of Philadelphia

- **Ben Goodman**
  President and CEO, 4A Security & Compliance

- **Rachel Greenstadt**, PhD
  Associate Professor, College of Computing & Informatics, Drexel University

- **Arun Lakhotia**, PhD
  Professor, Computer Science & Director, Software Research Laboratory, University of Louisiana at Lafayette


Space is limited—please register HERE as soon as possible.

**MONDAY, APRIL 13, 2015 1:15-5:00 PM**
Paul Peck Alumni Center 3142 Market Street, Philadelphia, PA

drexel.edu/cci

Figure 14: April 13, 2015 – Flier for the symposium “Balancing Act: Big Data, Cybersecurity, and Privacy”, co-organized by the Drexel Center for Visual and Decision Informatics and Drexel Cybersecurity Institute.
### Symposium & CVDI Industry Advisory Board Meeting Agenda
April 13 - 15, 2015
Philadelphia, PA

**Balancing Act: Big Data, Cybersecurity, and Privacy**

**Monday, April 13**

<table>
<thead>
<tr>
<th>Time</th>
<th>Activity</th>
<th>Presenters</th>
<th>Location</th>
</tr>
</thead>
</table>
| 1:15—1:30pm  | Symposium Opening & Introductions                                         | Dr. David Breen  
Deputy Director, CVDI and  
Associate Professor, Drexel University  
Dr. Steven Weber  
Director, DCI and Associate Professor,  
Drexel University | Paul Peck Alumni Center                                             |
| 1:30—2:00pm  | Keynote Talk                                                              | Mr. Keith Morales  
Assistant Vice President and  
Information Security Officer,  
Federal Reserve Bank of Philadelphia | Paul Peck Alumni Center                                             |
| 2:00—2:30pm  | **Big Data in Healthcare: The Promise and the Challenges of Privacy and Security** | Mr. Ben Goodman  
President and CEO,  
4A Security & Compliance | Paul Peck Alumni Center                                             |
| 2:30—2:45pm  | Break                                                                     |                                                                                                                                          |                                        |
| 2:45—3:15pm  | **Classify but Verify: Adversarial Stylometry and Machine Learning in an Open World** | Dr. Rachel Greenstadt  
Associate Professor, College of  
Computing and Informatics, Drexel University | Paul Peck Alumni Center                                             |
| 3:15—3:45pm  | **Harnessing Intelligence from Malware Repositories**                    | Dr. Arun Lakhotia  
Professor, Computer Science and  
Director, Software Research  
Laboratory, UL Lafayette | Paul Peck Alumni Center                                             |
| 3:45—4:00pm  | Break                                                                     |                                                                                                                                               |                                        |
| 4:00—5:00pm  | **Roundtable Discussion**                                                | Moderator:  
- Mr. Ben Goodman, 4A Security  
Panelists:  
- Dr. Rachel Greenstadt, Drexel  
- Dr. Arun Lakhotia, UL Lafayette  
- Mr. Patrick Lardieri, Lockheed Martin | Paul Peck Alumni Center                                             |
| 5:00—6:00pm  | Break/Travel to Davio’s                                                   |                                                                                                                                               | Davio’s  
111 South 17th Street  
Philadelphia, PA 19103 | Davio’s  
111 South 17th Street  
Philadelphia, PA 19103 |
| 6:00—9:00pm  | Symposium Reception                                                       |                                                                                                                                               | Davio’s  
111 South 17th Street  
Philadelphia, PA 19103 | Davio’s  
111 South 17th Street  
Philadelphia, PA 19103 |

Figure 15: April 13, 2015 – Agenda for the symposium.
Cybersecurity Practitioner Symposium
Thursday, February 19, 2015

1:00pm - Welcome & Opening Remarks

1:10pm - Keynote: Cyber - Why We’re Losing and What’s Needed to Win

Speaker: Steven R. Chabinsky
SVP of Legal Affairs, General Counsel and Chief Risk Officer, CrowdStrike,
Former Deputy FBI Cyber Division

2:00pm - Panel #1: Zero Trust Network Architecture
Network and standards requirements

Moderator: Sharon Goldberg
Assistant Professor, Computer Science Department, Boston University

Panelists:
Dr. Edward G. Amoroso, SVP and Chief Security Officer, AT&T
Alan Boehme, Chief of Enterprise Architecture, Coca-Cola
Chad Fulghum, Chief Strategy Officer, Tanium

2:45pm - Panel #2: Data Overload
Best practices for managing and harnessing the data overload

Moderator: Steven Weber
Associate Professor and Associate Department Head of Graduate Affairs,
Electrical and Computer Engineering Department, Drexel University

Panelists:
Firas Rifai, CEO and Co-Founder, Bay Dynamics
Myrna Soto, SVP and Chief Infrastructure and Information Security Officer,
Comcast
Lamont Orange, CISO, Vista Equity

3:30pm - Break

3:50pm - Panel #3: Authentication
Realities, requirements and timing for multi-factor and biometric authentication

Moderator: Rama Chellappa
Minta Martin Professor of Engineering, Chair of Department of
Electrical and Computer Engineering, University of Maryland

Panelists:
Sergio Rodriguez Jr., Chief Strategy Officer, The Credit Junction, Former
Financial Services Committee Professional Staff Member,
U.S. House of Representatives
Daig Song, CEO and Co-Founder, Duso Security
Cormac Herity, Principal Researcher, Microsoft Research

4:35pm - Fireside Chat: On the Horizon
Emerging cybersecurity innovations

Moderator: Dave Zilberman
Managing Director, Comcast Ventures

Panelists:
Mark Fernandez, Managing Director, Sierra Ventures
Alberto Yepes, Managing Director, Trident Capital

Please join us for a cocktail reception following the program.

This event is off-the-record.
UNITED STATES ARMY RESERVE

Cyber Private Public Partnership Strategic Vision

Chief of the Army Reserve #5 strategic priority: Sustain and enhance Total Army Capability through employer partnerships and an innovative force mix that facilitates movement of Soldiers between active and reserve duty across a Continuum of Service.

30 January 2015

Overview: The Army Reserve will be a major contributor to the Army and Joint Force of Cyber Security and Defenders in the near future. Successful long term USAR Cyber support to the Army requires development of a USAR Cyber Soldier pipeline for recruiting (new/current USAR Soldiers and transition AC Soldiers), training/education, employment in the Cyber Security profession, and education-training and research infrastructure (TRAIN AS YOU FIGHT).

The USAR Cyber Private Public Partnership was initiated in support of the Chief of the Army Reserve Private Public Partnership program (P3). The program is designed to emphasize the professional development, recruiting and retention of cyber security and cyber defenders in the Army Reserve. The Cyber P3 LOEs are mutually supporting to support individual, unit and leader readiness.

The US relies on information systems and data for almost every level of national power. US critical infrastructure and military operations are specifically at risk from Advanced Persistent Threats (nation-states, non-state actors, terrorists and criminal networks). The nature of cyber defense has shifted from passive defense, reliant on defense in depth and firewalls to active defense, with an emphasis on highly skilled and critical thinking cyber professionals. The demand for these individuals and units far outpaces the Cyber Soldier and unit inventory. The current DoD and Army school systems do not yet provide the throughput or advanced skills required for the USAR.

The Department of Defense has identified cyber security professionals as a critical shortage. The Reserve Component in a number of reports including, GAO and RAND (Hackers Wanted), identify the RC as a potential and immediate possibility to lessen the shortage of cyber security/defense professionals. The USAR stands at the threshold of providing significant and critical need to the federal government, DoD, public and private sector. This program is designed to understand, identify and fill a strategic opportunity for the USAR to provide an expandable, tailored and holistic solution for bridging the civilian and military cyber security capability gap.

Problem Statement: New threats and exponential expansion of cyber reliance and inter-connected critical systems creates a significant national security concern. The demand for Cyber Security professionals in the USAR and Army outstrips the inventory (40K in USG alone). Time constrained USAR Cyber Soldiers in this demanding and constantly changing military career field need to match civilian career skills to remain relevant and skilled. The USAR needs to establish a professional cyber security pipeline at each level; entry level, journeyman and master (that includes new Soldiers and transitioning AC Soldiers), that marries their civilian and military careers to provide continuous value to the Army and joint cyber demands. Future USAR strategy needs to consider 5-10 year time horizons to mature a Cyber Defense program that meets the nation’s requirements and maintains a critical qualified and experience USAR pipeline to units.

Program Objectives: Development of a successful USAR Cyber pipeline requires a comprehensive program that starts with Universities to build foundational and continuous cyber security education opportunities, civilian cyber employment opportunities to maintain skills, maintain relevance and recruit/retain the force and finally a shaping force that helps develop a generating force and potential candidate pool. The USAR Cyber P3 program provides clear value to attracting, generating, maintaining and retaining Soldiers because they see external value to the USAR and nation beyond just service in their units.

Program Purpose and Intent: The Cyber Private Public Partnership is intended to provide a catalyst for building Cyber security professionals and defenders in the USAR. It targets future recruits, initial entry soldiers, transitioning AC soldiers to USAR, prior service entering the USAR, existing USAR soldiers in cyber related fields and existing professional Cyber-soldiers. The program directly supports the recruiting, retention, transition and cyber skill progression of USAR Cyber soldiers across the USAR (Support, Operational and Functional Commands). Finally, the program is designed to provide a pool (individuals, units and leaders) of exceptionally qualified and experience Cyber soldiers that can support service, joint and interagency cyber events and operations. The aim is to bridge the civilian-military divide with mutually supporting careers and professional opportunities in cyber security.

Program Design: Program designed for close to 3500 - 5000 Army Reserve Soldiers

Figure 17: January 30, 2015 – Strategic vision of the United States Army Reserve for the Cyber Private Public Partnership.
Lieutenant General Jeffrey W. Talley
32d Chief of Army Reserve and Commanding General,
United States Army Reserve Command
cordially invites you to attend a

Private Public Partnership Cybersecurity Reception
on Tuesday, the tenth of February, two thousand and fifteen
at five o'clock in the evening
2168 Rayburn House Office Building
Captiol Hill
Washington, D.C. 20515

R.S.V.P. by 6 February 2015
POC: Sheila Drees
703-695-0409

Military: Duty Uniform
Civilian: Business Casual

Click Here to R.s.v.p.

Figure 18: February 10, 2015 – Invitation for the signing ceremony of the Memorandum of Understanding between Drexel University and the United States Army Reserve for the Cyber Private Public Partnership.
United States Army Reserve
Private Public Partnership
Cyber-Security Reception

February 10, 2015
Rayburn House Office Building
Washington, D.C.

Hosted by
Lieutenant General Jeffrey W. Talley
32nd Chief of Army Reserve
Commanding General, United States Army Reserve Command

Sequence of Events

Opening

Program Description

Introduction of VIPs

Remarks by
Lieutenant General Jeffrey W. Talley

Signing

Conclusion of Ceremony

Reception immediately following

University Partners
University of Colorado Colorado Springs
Drexel University
George Mason University
Norwich University
University of Texas at San Antonio
University of Washington Tacoma

Employer Partners
AECOM Management Services
CALIBRE Systems, Inc
Chevron Corporation
DynCorp International
EMC Corporation
Federal Bureau of Investigation
Microsoft
Professional Project Services (Pro2Serve)
Rackspace USS, Inc
T-Mobile USS, Inc
Verizon

Figure 20: February 10, 2015 – Agenda for the signing ceremony.
The United States Army Reserve (USAR) works tirelessly to increase the overall readiness of Soldiers in order to support crucial national initiatives in times of peace and war. The Army Reserve created the Private Public Partnership (P3) Office to facilitate strategic and mutually beneficial relationships with employers, universities, and organizations to ensure comprehensive support for Soldier readiness. Members of the P3 Cyber Initiative are uniquely suited to provide critical training and employment opportunities to members of the USAR. Jointly, the USAR, and its Employer and University Partners enter into this statement of support to facilitate a strategic and mutually beneficial relationship and encourage the exploration of cyber initiatives providing America’s Warrior-Citizens and Veterans with employment and training opportunities.

The undersigned are representatives of each Phase I entity, university and employer partner, that support the USAR and P3 in the mission to educate and employ cyber Soldiers.

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeffrey W. Talley</td>
<td>Lieutenant General, U.S. Army Reserve</td>
</tr>
<tr>
<td>Evan Guzman</td>
<td>Verizon</td>
</tr>
<tr>
<td>Mark DeCrafft</td>
<td>Professional Project Services</td>
</tr>
<tr>
<td>Jaylee Turgell</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>Thomas Mullen</td>
<td>FMC Corporation</td>
</tr>
<tr>
<td>John Engates</td>
<td>Rackspace US, Inc.</td>
</tr>
<tr>
<td>Bill Boni</td>
<td>T-Mobile US, Inc.</td>
</tr>
<tr>
<td>Martin Wood</td>
<td>University of Colorado Colorado Springs</td>
</tr>
<tr>
<td>Marla Weisz</td>
<td>Drexel University</td>
</tr>
<tr>
<td>Dr. Kenneth Ball</td>
<td>George Mason University</td>
</tr>
<tr>
<td>Gordon Sullivan</td>
<td>Norwich University</td>
</tr>
<tr>
<td>Dr. John Frederick</td>
<td>University of Texas at San Antonio</td>
</tr>
<tr>
<td>Dr. Kenyon Chan</td>
<td>University of Washington Tacoma</td>
</tr>
<tr>
<td>Theodore Dyer</td>
<td>DynCorp International</td>
</tr>
<tr>
<td>Ronald Hahn</td>
<td>AECOM Management Services</td>
</tr>
<tr>
<td>Michael Martin</td>
<td>CALIBRE Systems, Inc.</td>
</tr>
<tr>
<td>Christopher Lukas</td>
<td>Chevron Corporation</td>
</tr>
<tr>
<td>Christopher Cornez</td>
<td>Microsoft</td>
</tr>
</tbody>
</table>
Figure 22: February 10, 2015 – Lieutenant General Jeffrey W. Talley signing the Memorandum of Understanding for the United States Army Reserve for the Cyber Private Public Partnership.
Figure 23: February 10, 2015 – Signatories of the Memorandum of Understanding for the United States Army Reserve for the Cyber Private Public Partnership.