Proposal for:

CyRes

University of Pittsburgh

***Cy*ber Security, Privacy, Trust and Resilience *Res*earch Center**

The name of:

- Individuals initiating proposal:

  Ronald L. Larsen, Dean and Professor, School of Information Sciences (SIS)

- Responsibility Centers:

  School of Information Sciences,
  University of Pittsburgh

- Center to be developed:

  Tentative names (to finalize)
  UP Center for **Cy**ber Security, Privacy, Trust and Resilience **Re**search (CyRes)
  Center for Cybersecurity Research
  Center for Research for Security, Privacy and Trust (CReSPT)

  NOTE: Tentatively, "CyRes" has been used in the document. While cyber security is a popular term used, we use it in this document to refer to *security*, *privacy*, *trust* and *resilience* in general.

d) Schools/Departments affected

The center is expected to have affiliated faculty members from (at least initially)

School of Information Sciences
Dietrich School of Arts and Sciences
    Departments: Computer Science, Mathematics, Philosophy, Psychology
School of Law
School of Health and Rehabilitation Sciences
    Department: Health Information Management
Swanson School of Engineering
    Departments: Electrical Engineering, Nuclear Engineering
Graduate School of Public and International Affairs
School of Nursing

External Partners: UPMC, NCFTA, CMU CyLab

- Date Submitted:

Table of Contents

1. Introduction

The rapid growth of Information and Communications Technology (ICT) has enabled unprecedented opportunities for innovation, commerce and social transformations. Individuals, organizations and nations are now ever more dependent on the fast evolving digital infrastructures that are intricately interconnected. Protecting such ICT infrastructures and the information that is stored and processed in them has become a significant concern because of the potential damage that security and privacy breaches can cause to individuals, organizations, and nations. The rapidly growing frequency and severity of cyber-attacks and cybercrimes that are both *disruptive* and *destructive* in nature are well-documented and they pose significant threats to national and economic security, and the well-being of our society. The Internet of Things (IoT), big data, smart and resilient cities/planet, cloud/fog infrastructures, etc., are recent ICT developments that are making cyberspace ever more complex and significantly increasing the attack surface. Further, the regulatory and legal boundaries across different geographic regions introduce significant challenges to handling cyber crimes and intrusions and establishing trust boundaries to guide cyber security responses. Besides innovative cyber security solutions, there is a critical need to develop novel and pragmatic approaches to mitigate risks and make cyberspace more resilient. There is an urgent need for accelerated and highly multidisciplinary and translational cyber security research to generate solutions that are foundational, holistic and easily deployable as systems, tools, techniques and/or methodologies [Pnen]. Pitt is uniquely positioned to leverage its strengths to become a leading place for such holistic, multidisciplinary research in cyber security.

This proposal aims to establish a cyber security research center at the University of Pittsburgh whose goal will be to foster highly integrated, holistic and interdisciplinary undertakings that push the boundaries of cyber security research and development. It will leverage and build upon the synergies that exist among various units within Pitt. The center will focus on both basic research and contributions to solving real-world cyber security, privacy, trust and resiliency related challenges.

Pitt can establish a truly multidisciplinary and holistic cyber security research agenda. In particular, various prominent engineering centers/programs (Energy, Nuclear, Manufacturing, RFID, Medical innovation, etc.), policy focused centers/programs (GSPIA, Ridgeway, CoNP, CoDM, etc.), healthcare programs (UPMC, HIM, Nursing, DBMI, etc.), and other academic units (Business, Social Sciences, Math, Philosophy, etc.) provide tremendous opportunities to help carry out more holistic cyber security research.

Below, we overview current cyber security efforts at Pitt, present the proposed center, discuss organization/management and budgetary sides, and compare it with some key other academic centers focused on cyber security.

2. Background: Cybersecurity Landscape & Pitt's Current Efforts

2.1 Cyberattacks and Cybercrimes

Recent cyberattacks, such as the Target breach, Sony hacking incident, BlackEnergy malware, Anthem cyber-attack, the Chinese hacking incidents, etc., show how vulnerable individuals, organizations, and nations have become against malefactors with intent and will to inflict damage. In 2009, hackers broke into Wal-Mart and stole information from cash registers [1]. Home Depot's system was hacked in 2014, and credit card numbers of its 60 million customers were stolen. The well-known Target breach is

estimated to have incurred a loss of $148 million. In 2014, iCloud accounts, in particular those of Hollywood celebrities, were compromised to expose socially embarrassing pictures. The same year, retailer Neiman Marcus was a victim of cyberattacks that involved illegal access to customer credit card information. JP Morgan Chase was another big victim of cyberattacks [1]. The Sony hacking incident further exposed the global nature of the cyber attacks from state actors, and its multifaceted and long-term impact. Earlier in 2011, Mandiant's report on Chinese state sponsored cyber attacks on various high profile companies (with three from the Pittsburgh area) painted a grim picture of the significant damages that can be done in cyberspace [7]. *Threat actors* included: 45.6% cyber criminals, 17.45% nation/state actors, 19.81% hacktivists, 40.09 % hackers, 28.62% malicious insiders, and 40.72% non-malicious insiders [2],.

Healthcare sectors are increasingly vulnerable to cyber attacks. According to the survey in [3], only about 53% of healthcare providers indicate their readiness to defend against a cyber attack. Four-fifths of people in executive positions in health care provider and payer institutions indicate that their IT environments have been compromised. Cyber attacks can lead to financial fraud, medical insurance fraud, compromise of computer-controlled medical devices, and patient privacy [3]. Key concerns from providers include cost for regulatory enforcement, litigation, financial loss, reputation, etc. A report from Atlantic Council indicates that the security breaches reported by healthcare providers increased 60% from 2013 to 2014, with a 282% increase in financial losses [8]. In March, the Washington Post reported that "*2015 is already the year of the health-care hack*" [20].

The protection of ***critical infrastructures*** is a growing concern for national security. Attacks from insiders and external threat agents that are *persistent* are seen as potential disasters if solutions to mitigate them are not urgently pursued. In 2014, *Industrial Control System Cyber Emergency Response Teams* (ICS-CERT) released an advisory that BlackEnergy malware/crimeware that exploits human-machine interfaces has compromised several ICS environments. Use of the Stuxnet malware in Iran nuclear power plants to control the working of nuclear processes shows the dangers of cyber security incidents on ICSs. ICS-CERT reports that cyber attacks on critical infrastructures are rapidly increasing, with 55% of investigated incidents showing signs of *advanced persistent threats* or targeted attacks. In 2014, a Russian hacker group used a malware called Havex to break into ICS/SCADA systems – primarily in energy sectors. Another example is that of the Ugly Gorilla malware from a Chinese attacker that targeted the ICSs of utilities. Stuxnet, Havex and BlackEngery malware indicate huge cyber security efforts in terms of time and money. With critical infrastructures increasingly dependent on the Internet, they are being exposed to increasingly easier attacks from anywhere and by anyone. Further, critical infrastructures such as dams [21], and nuclear power plants are "*insecure by design*," [], thus, exacerbating the situation.

In addition, cyber bullying incidents and other privacy exposures present stark picture of how cyberspace has encroached into personal lives and society []. There is also significant growth of ransomware (e.g., 500% growth from 2012 to 2013), social media scams, and malware in mobile devices.

2.2 Cybersecurity Costs and Funding

The concerns for cyber security and its economic impacts have fueled funding for R&D and education in this area. In early 2015, the Secretary of Defense released the DoD's Cyber Strategy, where it was emphasized that " ... *the scale of the cyber threats requires urgent action*" towards building capabilities for cyber defense and cyber operation. President Obama has allocated $5.5 billion for DoD's cyber infrastructure operations and maintenance programs [4]. A total of $14 billion has been designated for cyber security in the 2016 budget by the President – which is an increase of 10% from that of 2015. NSF's estimated funding for SaTC, the mainstream program for cyber security at NSF, is $124.25 million

(1.2% increase from last year) []. In addition to SaTC, NSF CyberCorps represent NSF's emphasis for cyber security education and research – with a projected budget of $45 million. Besides these, various other NSF programs such as CNS, IIS, Smart Health and Well-being, and Expedition in Computing provide other opportunities. Similar funding opportunities are also channeled through other federal agencies (e.g., Army, Navy, DoE, DHS, DoJ. NSA, etc.). Appendix C lists some recent BAAs that have included significant funding opportunities recently.

Cyber security initiatives from the government, such as NSA/DHS's center of academic excellence (CAE) programs including, CAE IA-Cyber Defense, CAE-Research, CAE Cyber Operations, CAE Forensics, etc., NIST's NICE (National Initiative for Cyber security Education) highlight the growing emphasis the US has placed in cyber security research and education.

2.3 The Urgent Need for Cybersecurity Research

Overall, there is a significant growth of cyber attacks and crimes, and the economic and social impacts are very worrisome, raising significant need for accelerated research in cyber security areas. It is critical to develop holistic and multi-disciplinary cyber security approaches geared towards addressing the rapidly increasing sophistication of cyber threats. Cyber security is not only a technical issue. Both technical and non-technical solutions need to be synthesized to produce holistic cyber security solutions. Cyber security requires multi-faceted solutions encompassing technical, policy, legal, ethical, and social dimensions. Cyber security solutions need to satisfy legal and regulatory requirements which themselves vary from state to state and country to country, and they need to be acceptable to individuals and societies with diverse cultural values. The global connectivity and multi-jurisdictional issues significantly complicate cyber borders and pose difficulties in mitigating and handling cyber crimes. Thus, holistic and highly multidisciplinary approaches are needed to effectively and efficiently tackle increasingly sophisticated cyber security incidents that cross geographic and jurisdictional boundaries. The proposed center will be founded on the knowledge of these various key characteristics of the cybersecurity landscape. Such research should be founded on the proper understanding of the various underlying cyber security and privacy issues/characteristics, such as, but not limited to, the following:

(i) **Interconnectivity**: ICT infrastructures, sensors, systems, devices, etc., are increasingly connected in cyberspace. Such connectivity significantly widens the threat landscape and increases the attack surfaces. Interconnectivity means the infrastructures/systems are only as secure as the weakest links. In particular, each element in this *Internet of Things* (IoT) may have inherent vulnerabilities, many of which may be unknown a priori and thus easily exploited by attackers. Tremendous heterogeneity of devices/sensors, protocols, software components, regulatory and legal requirements, policies, etc., make security, privacy and trust challenges extremely difficult to tackle in a holistic way. Software and hardware components in the ICT environments are produced by manufacturers/providers/suppliers that form an intricate, globally distributed supply chain. Such supply chain environments exacerbate insider threats, while providing numerous paths for an attacker to exploit. Tracing back cyber criminals, and even establishing trusted cyber borders/boundaries to deal with cyber incidents has become a herculean task.

(ii) **Rapid Evolution**: Information technologies are frequently updated and newer systems quickly make older ones obsolete. Further, the environments (e.g., healthcare, power grid, and nuclear power plants) where ICTs are deployed are themselves changing and evolving to accommodate newer services, requirements and/or regulations. The co-evolution of cyber and non-cyber components

within an environment can be significantly out of sync. For instance, the non-cyber parts of a nuclear power plant generally evolve much more slowly than the cyber components do. In the rapidly evolving environments, even a small change can have significant impact on the overall attack surface, e.g., by introducing newer, unknown vulnerabilities. Further, some of these changes may include incorporating completely new paradigms that need to co-exist with older ones (e.g., recent emergence of the cyber-physical systems (CPS), IoT, Cloud/fog computing paradigm). These generate different types of cyber security, privacy and trust concerns, and constantly demand significant and rapid rethinking of existing solutions.

(iii) **Increasing Threats and Sophistication of Attacks**: Adversaries are getting smarter, better organized and more persistent, with access to a huge arsenal of automated tools and computing resources. Further, there are various motivations including individual financial gain, cyber espionage, hacktivism, nation-state cyber wars, and cyber terrorism. Tools are increasingly available freely over the web. These enable motivated and persistent attackers to easily constructing clever and novel attacks that can have dire consequences.

(iv) **Humans Factors & Usability**: Humans have been recognized as a very weak links with regards to cyber security of the increasingly interconnected digital society. Humans provide an easy way for cyber-intrusions and disruptions and are increasingly being targeted (e.g., through phishing and social engineering attacks). It is a huge challenge to keep up with the fast paced cyber evolution, including changing cyber security solutions. This generates significant challenges in developing effective solutions that can be easily configured and used from a human factors perspective. Often, a lack of usable design translates into increased threats because of the lack of proper understanding and/or ease of use of available, effective solutions.

(v) **Information Explosion, its Ubiquitous Flow and Aggregation**: Increasingly all types of information in huge amounts are readily available in the cyberspace. First, this introduces significant data security, privacy and quality issues, as well as digital curation and provenance challenges. Secondly, various pieces of publicly available information can be aggregated to infer high value information, and leveraged to construct effective attack vectors (e.g., background information can be used for privacy attacks in social networks). The accelerated growth of information continues while current challenges are far from being solved.

2.4 Current Cyber Security Efforts at Pitt

While there have been cyber security research efforts in various schools and departments, the most concentrated efforts have been through faculty from various departments affiliated with the *Laboratory for Education and Research on Security Assured Information Systems* (LERSAIS), within SIS. Other faculty, notably those in GSPIA have cyber crime and security intelligence related research interests.

The School of Information Sciences (SIS) launched its Cyber security education and research program in 2003 with the hire of James Joshi. Under his leadership and the support of three other SIS faculty members, Michael Spring, Prashant Krishnamurthy, and David Tipper, the LERSAIS opened its doors in 2004. James Joshi is the Director of LERSAIS. The CS department hired cyber security faculty Adam Lee in 2008. Faculty members from the CS department who are affiliated to LERSAIS include Adam Lee, Daniel Mosse and Taieb Znati. Recently, Balaji Palanisamy has joined LERSAIS as an additional tenure track SIS faculty member. David Thaw is another expert in cybercrime who recently has joined Pitt with

joint appointments in SIS and School of Law. Eric Hatleback is a research associate professor affiliated with LERSAIS with joint appointments at CERT and SIS. Another key faculty with significant cyber security interests is Alex Jones in Computer Engineering department.

The central goals of LERSAIS included establishing a premier research program in cyber security and developing high quality cyber security education. LERSAIS has been designated a National Center of Academic Excellence in Information Assurance Education (CAE) since 2004 and was among the first group of institutions to be designated a CAE-Research (2008). Both the CAE and CAE-R programs are jointly managed by the Department of Homeland Security (DHS) and the National Security Agency (NSA). Receiving the designation includes going through a rigorous application and program review process. Pitt is one of 15 CAEs in the U.S. whose cyber security curriculum has been certified to meet five Committee on National Security Systems (CNSS) standards for IA education. Recently, LERSAIS has been re-designated as both a CAE and a CAE-R until 2021 under newly revised criteria. Aligned with the NSA's CAE programs, the LERSAIS team has consistently maintained an active portfolio of research and education activities. Key milestones achieved by LERSAIS include:

- 2003: (December) – received certification for CNSS 4011 Information Systems Security Professionals and CNSS 4013 Systems Administrators in Information Systems Security
- 2004: (February) – received certification for CNSS 4012 Designated Approving Authority
- 2004: (April) – received the NCAE/IAE designation for the University jointly from NSA and DHS, with 5 CNSS certifications
- 2004: (July) – received $286,710 NSF-SFS Award # 0415761 (Scholarship for Service) for SAIS course development
- 2006: NSF-SFS Scholarship award to establish CyberCorp scholarship program to educate Cybersecurity graduates
- 2008: Among the first to receive the CAE-Research designation from NSA/DHS (research intensive IA programs)
- 2011: NSF-SFS Second Round of scholarship program funding awarded
- 2014: HP-sponsored survey ranked Pitt cybersecurity program 7th in the nation. Re-designation of LERSAIS as CAE & CAE-Research. Funding to create a "Security Assured Health Informatics" curriculum in collaboration with the department of Health Information Management at the School of Health and Rehabilitation Sciences. Collaboration with SEI/CERT on the Science of Cybersecurity (joint funding from Pitt and SEI to support a research associate professor)

Visibility of Pitt's Cybersecurity efforts has been seen in public over last several years. Notable among these include the following public rankings of cybersecurity programs in the country:

- ***ExecutiveBiz*** ranks Pitt at the 6th place for "Preparing Cybersecurity Professionals" (http://blog.executivebiz.com/2009/09/top-10-universities-preparing-future-cyber-security-professionals/).
- ***HP sponsored Ponemon*** study ranks Pitt in the 7th position in "2014 Best Schools for Cybersecurity";

  (http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf)
- ***ObserveIt*** site ranks Pitt's LERSAIS at the 6th position among the recommended cyber security programs in US.

(http://www.observeit.com/blog/7-universities-recommend-security)

LERSAIS affiliated faculty members James Joshi and Adam Lee have received *NSF CAREER* grants on cyber security and privacy projects. Affiliated LERSAIS members have received support from NSF, DoD/NSA, DARPA, etc., as well as from industry such as Cisco. More information on LERSAIS-related activities can be found at: http://www.sis.pitt.edu/lersais/.

It is to be noted that the key cyber security faculty hires at Pitt essentially include: James Joshi, Adam Lee, Balaji Palanisamy and David Thaw. Prashant Krishnamurthy and David Tipper have significant interest in CyRes relevant research. Other faculty members affiliated to LERSAIS mentioned above have varying degrees of interest/efforts in cyber security research, often depending on funding status. LERSAIS organizes distinguished IA seminar every Fall and Spring semesters since 2004 (over 60+ seminars so far). Lists of LERSAIS research/education grants and PhD students who have completed their studies are included as Appendices A-B.

Several other centers at Pitt have focused activities related to some aspects of cyber security, mainly in the policy and legal domains. These include *Mathew B. Ridgway Center for International Security Studies* that is focused on policy and international cybercrime, and *Pitt's Center for National Preparedness*, which is a broad, multidisciplinary, collaborative enterprise that engages the University's scientists, engineers, policy experts, and clinical faculty.

While we have maintained a high level of productivity and visibility, we need to significantly enhance both the depth and breadth in faculty expertise in cyber security to become the best place for holistic and multidisciplinary cyber security research.

3. The Proposed Center: Vision & Strategic Goals

We propose to establish a *University of Pittsburgh Center for **Cy**ber Security, Privacy, Trust and Resilience **Res**earch (CyRes)* that is founded on the understanding of cyber security characteristics/challenges mentioned earlier. ***Holistic and highly multidisciplinary research will be the key focus of the proposed center***.

3.1 Vision & Strategic Goals

Vision: *The Center* will be a global leader for inter-disciplinary research related to security, privacy, trust, and resilience in cyberspace. It will be among the best cyber security research centers in the world and will be founded on the principles of:

- Integration and cross fertilization of scientific, engineering, technological, policy, legal, business, sociological and human perspectives
- Service to local, regional and global communities by research outreach and research-driven training, awareness and education
- Collaboration and partnership with synergistic entities in academia (within and outside Pitt), both public-private sectors, and global partners.
- Agile and efficient environment that seamlessly supports bold and high-risk research explorations.

Strategic Goals: To realize the above vision, we set the following strategic goals:

1. The center will develop a critical mass of core researchers that will represent both breadth and depth in various research areas related to cyber security, privacy, trust and resilience.

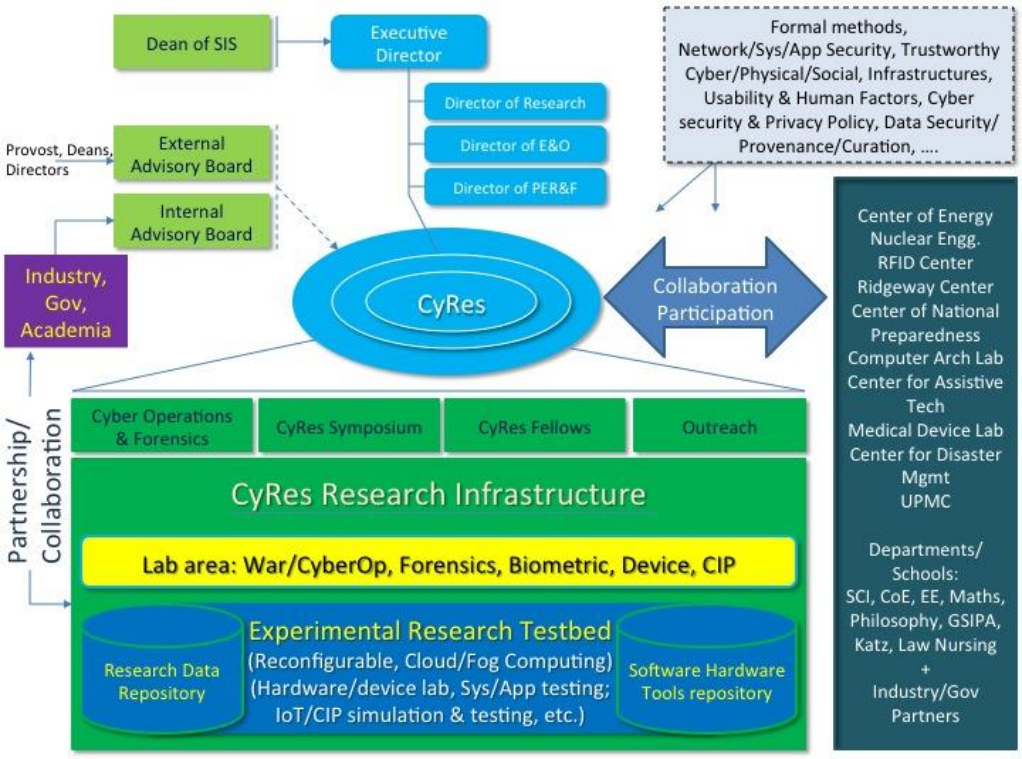
   The center will facilitate and foster multidisciplinary collaborations among faculty within the University by exploiting the synergies that exist, and by exploring new opportunities. *We will create **high priority areas** in a timely manner to streamline multidisciplinary research efforts in these areas so as to generate significant momentum early on.*

2. The center will provide foundational support to affiliated faculty to explore and establish closer collaborations with other research institutions/centers (academia, industry and government institutions) locally as well as globally to enable innovation and exploration in relevant research.

3. The center will establish a seamless, holistic infrastructure to enable affiliated researchers and groups to serve local, regional, and global communities in cyber security and cyber defense/operations with regards to state-of the art research, training and education. Such a holistic infrastructure will include:

   a. a state-of-the-art technical research infrastructure,
   b. an outreach infrastructure, an infrastructure for translating research into deployable prototypes, processes/methodologies and tools, and
   c. an infrastructure for research outcomes driven education, training and awareness.

   Towards goals 2-3, two key activities that we will also emphasize will be: (i) *Annual CyRes Symposium*; and (ii) *CyRes Fellows program*.



The Proposed CyRes Center

Figure 1 overviews the proposed CyRes center. Below we discuss various components of the center.

3.2 Research Agenda

The breadth of relevant research will include, but are not limited to the topics listed in Table 1.

Table 1. Cybersecurity Research Topics

Key Cyber security & privacy Research topics	Examples
Foundational theories/techniques research	e.g., formal models and methods, composability and verification, secure & trusted interoperation, cryptography and number theory, quantum cryptography, etc.;
Systems and hardware oriented research	e.g., secure processors, secure OSs, static/dynamic analysis techniques; secure software engineering or software security; secure medical devices/RFIDs
Secure and resilient Network focused research	e.g., wireless networks; secure SDN, DDoS mitigation, secure SDN,
Trustworthy cyberinfrastructure focused research	e.g., wireless networks; secure middleware; secure mobile infrastructure, security of Internet of Things/Everything infrastructure, etc.
Application focused and applied research	e.g., those related to healthcare/bioinformatics applications, database applications security and privacy, social network applications, mobile app security, etc.
Data centric security, privacy and trust research	e.g., that relates to big data security, secure data mining, secure knowledge management, anonymization techniques, data provenances and digital curation, etc.
Security, Privacy and Resilience of Cyber physical systems & Cyber social/human systems	e.g., related to critical infrastructure protection – SmartGrid security, Nuclear Cybersecurity, Transportation infrastructure security; internet of medical devices, vehicular cybersecurity, secure and resilient Smart Cities/Planets; Cyber bullying, Hactivisim, Secure and resilient disaster management, etc;
Cyber Intelligence Analytics, Cyber Operations and Forensics	e.g., intelligence data gathering/fusion and analytics for real-time detection (data driven approaches: DDoS, Honeypots, etc.), digital forensics research, CyberOp methodologies and simulation environments (war room), etc.
Trustworthy Computing Paradigms	e.g., relevant to Cloud computing, fog computing, quantum computing, high performance computing, etc;
Human Factors and Usability research in Security and Privacy	e.g., User-centric Privacy policy design/engineering; Usable Interfaces, Phishing and spam control/mitigation, Social engineering attacks, Insider behavioral modeling etc.,
Threat Modeling, Risk Management and Security Metrics	e.g., modeling of insider and outsider threats, supply chain security, quantitative techniques, risk assessments and security metrics/measurement, social engineering threats, understanding and managing advanced persistent threats;
Cyber Security and Privacy Policy, Regulations, Legal and Ethical issues	e.g., Security and privacy laws/regulations (e.g., HIPAA, etc.), Compliance tools/techniques, Multi-jurisdictional cyber crime investigation, Cyber border, etc.
Science of Cyber security	e.g., reproducible experimentation, basic laws for cybersecurity, etc.

Pitt has several centers and groups that have been leaders in research domains that overlap with these research areas. These include to name a few examples the Center of Energy, RFID center of excellence, UPMC. Efforts to exploit the synergy with these centers/units/groups will be a focal point for hiring accomplished cyber security faculty members to create a core group of faculty.

In Figure 1, the inner CyRes oval represents the group of core CyRes researchers who have expertise in the research areas list above and who spend most of their time in cybersecurity research (e.g., 50% or more of their research efforts). The middle oval represents CyRes researchers who have strong research activities in CyRes domain but their primary research focus may be another research area. The outer oval represents the group of researchers whose primary focus is another area but have some interest in CyRes domain.

3.2.1 Target Research Areas

The center will strive for agility in initiating or creating new research directions and generating strong research momentum in these directions ahead of the peers. Initial targets for research will be:

- ***BigData Security & Privacy***: Pitt has already established a strong foothold in the Big Data area, with several departments focusing on closely related research. SIS has launched a Big Data track of study. Big Data analytics provides a set of tools to address challenging problems. Big Data applications in areas such as business introduce daunting technical and non-technical challenges with regards to security and privacy. The proposed center will provide a platform for cross-fertilization of Big Data and Security/Privacy research activities. These include exploring synergies among Pitt researchers focused on cloud computing, social informatics, Internet of Things/Everything, biomedical informatics, to name a few. Some examples of initial efforts from LERSAIS affiliated faculty members address privacy issues in social networks and location based services (e.g., access control and anonymization) and security and privacy of cloud infrastructures (e.g., access management and privacy-conscious processing of huge amounts of data in the cloud).

- ***Security, Privacy and Resiliency of Healthcare IT Environments***: Healthcare IT environments present significant security and privacy challenges (e.g., privacy requirements of patients and the need to protect access to, and usage of, research data). Further, innovation in medical devices and related communication protocols linking devices to networked applications, and Big Data applications yield a rich, converged environment requiring innovation in security and privacy. LERSAIS affiliated researchers have partnered in large proposals aimed at integrating research in medical devices at Pitt's RFID Center of Excellence and in telemedicine research with the Health Information Management (HIM) department (in SHRS). Such opportunities are increasing and Pitt's strength in medical/healthcare research presents a unique opportunity for pursuing breakthrough research in this area. CyRes will closely align with the Data Alliance initiative. CyRes will focus on enabling collaboration and coordination needed to support the research efforts.

  Focus on this sub area also directly aligns with Pitt's institutional strategic research goal of 'Personalized Healthcare".

- ***Security, Privacy and Resiliency of Critical Infrastructures***: As discussed earlier, protection of critical infrastructures has become a national security issue. Pitt has significant and leading presence in critical infrastructure areas such as SmartGrid, Nuclear Engineering, Transportation, Manufacturing, etc. Through the proposed center, we can ensure highly multidisciplinary efforts to make high impact research contributions towards national security by making foundational contributions that help protect critical infrastructures. Some initial collaboration is contributing to grant proposal writing efforts related to cyber security for nuclear power plants. Some collaborative efforts are being pursued in SmartGrid security area as well. Several other opportunities within other domains such as Manufacturing, Transportation, Internet of Things/Medical Devices, 3D printing, etc., exist within Pitt as another unique set of opportunities.

- ***Cyber Intelligence Analytics & Digital Cyber Forensics Research, and Cyber Security & Privacy Laws/Regulations***: With plethora of cyber incidents, the challenge is to devise real-time defense opportunities to prevent potential attacks. Extensive, data-driven and efficient approaches are urgently needed to enable effective real-time detection and defense. Pitt currently does not have an established set of cyber security intelligence analytics research efforts, however, there is some initial movement towards this. One immediate goal of CyRes will be to streamline efforts in this area. Similarly, after the fact analytics for fast assessment of cybercrimes and establishing proper evidence for effective handling of global cyber incidents is increasingly becoming critical. With local potential partners such as NCFTA and SEI-CERT, this area has a significant practical relevance as well as national urgency. Further, this sub area requires multidisciplinary research because of the global nature of

cyberspace and cybercrimes. CyRes research with colleagues in other units such as Ridgeway Center and Center for National Preparedness, Law, and GSPIA will allow Pitt to uniquely pursue breakthrough research in this direction.

- ***Privacy Engineering, Data Curation, Archiving & Provenance, & Societal Aspects of Cybersecurity***. Privacy is emerging as a next generation challenge – that requires technical as well as legal, regulatory and legal dimensions. Currently, technical approaches to privacy have been pursued by various LERSAIS affiliated research. However, significant multidisciplinary research momentum is critical to be a leader in this critical and emerging space. Within SIS as well as other units at Pitt, there is also growing potential for related security and privacy research with a direct impact on individuals and society. For instance, SIS has substantial expertise in cyber bullying, protection and provenance of digital archives, information ethics, and intellectual property policies, etc. Digital archiving presents significant challenge with regards to protection of individual's privacy over the lifecycle of his related digital information.

- ***Other Sub Areas***: Many other sub-areas will be explored for strategically positioning Pitt for prominence. Some examples include:

    - ***Science of Cybersecurity***. With seed funding from the Office of Research, a new collaboration with SEI/CERT and the Department of History and Philosophy of Science is currently providing a unique opportunity to develop a highly speculative Science of Security.

    - ***Quantum Cryptography and Security***. Pitt's well-known Quantum information processing research is a potential big player in security arena in near future. Collaboration among cybersecurity researchers and Quantum computing researchers is unexplored territory at Pitt and has a potential for unique set of breakthroughs.

    - ***Hardware/Device Security***: Unique opportunity is also present at Pitt to pursue hardware level security. Pitt's strong presence in the domains of RFID research, medical devices, computing architectures, etc., provides opportunities to pursue breakthrough research towards developing efficient and effective novel hardware based/level security and privacy solutions. Such solutions (e.g., Physically Unclonable Functions) can provide a foundation of the overall system environment.

    - ***Biometric Authentication***. Authentication is a fundamental aspect of security and is increasingly becoming more important. Innovation in biometric authentication approaches that are effective, efficient and non-intrusive is critical in increasingly ubiquitous IoT environments.

3.3 Leadership, Membership and Staff implications

The center will be part of the School of Information Sciences. The Center reports to the Dean of the School of Information Sciences for administrative purposes, including:

- Budget approvals
- Approval of personnel hiring, firing, promotion or other personnel adjustments affecting the Center
- Approval of all center related administrative and strategic decisions

- Review of operational decisions

The Center will obtain guidance and vision from an ***External Advisory Board*** (EAB) with members from *Industry*, *Academia* and *Government*. Leadership and development of new initiatives will be conducted in consultation with an ***Internal Advisory Board*** (IAB), which will include representation from the Provost's office and Deans or chairs of affiliated units or their appointees

The initial leadership for the Center will include:

- **Center Director (or Executive Director)**:
  - Will have the overall responsibility of the center in establishing strategic research directions and agenda for the center as well in overseeing its operation.
  - The person in this role is expected to be a very well established, highly visible and core CyRes faculty member; ideally he will be a full Professor at Pitt, with a distinguished track record of highly impactful research and education.

The Executive Director will be supported by the following individuals in leadership roles:

- **Director of Research**
  - Help develop the overall research strategy and leads efforts in achieving operational and tactical goals related to the research strategy;
  - Understands research capabilities of faculty/staff affiliated with the center and also collaborate with several of them;
  - Tracks current and past research activities and identifies existing and emerging synergies among affiliated researchers;
  - Coordinates activities to seek new research directions and opportunities and facilitate the creation of newfound collaborations
  - He will be a tenured faculty at Pitt

- **Director of Education and Outreach**
  - Develops the center's strategy for education and outreach and channels CyRes faculty's recommendations to the educational degree programs
  - Manages current and emerging cyber security educational partnerships within the university (e.g., Cyber security education legal track, cybercrime and intelligence track, health IT assurance track, Critical infrastructure systems security track, etc.)
  - Leads development of educational partnerships (e.g., other external partners, K-12 outreach, community colleges, etc.)
    - External partnerships will be broadly sought out, including local community (NCFTA, SEI/CERT, Local industry, etc.), academic partners like CMU, RMU, Duquesne, Purdue, GeorgiaTech, etc.)
  - Preference will be for a tenure stream faculty at Pitt.

- **Director of Industry Partnerships, External Relations and Finances**
  - Builds corporate and government partnerships for research and education and relationships with external entities that enhance the strategic goals of the center
  - Fosters industrial sponsorship in support of education and research goals
  - Coordinates grant writing activities and team work
  - The person appointed to this position is not required to be a faculty member.

Table 1. List of Pitt Faculty members relevant to CyRes (Initial listing)

School of Information Sciences	**James Joshi, Professor**
	Prashant Krishnamurthy, Associate Professor
	Balaji Palanisamy, Assistant Professor
	Konstantinos Pelechrinis, Assistant Professor
	Michael Spring, Associate Professor
	David Tipper, Associate Professor
	Vladimir Zadorozhny, Associate Professor
	Eric Hatleback, Research Associate Professor
School of Arts and Sciences:	**Adam Lee, Associate Professor**
Department of Computer Science	Rami Melham, Professor
	Daniel Mosse, Professor
	Taieb Znati, Professor
	Youtaou Zhang, Associate Professor
Department of Mathematics;	Kiumars Kaveh, Assistant Professor
Department of Philosophy	---
School of Health and Rehabilitation Sciences: Department of Health Information Management	Bambang Parmanto, Professor
	Leming Zhao, Assistant Professor
School of Law	David Thaw (Secondary appointment with SIS)
School of Engineering: Nuclear Engg Program	Daniel Cole, Associate Professor
Department of Electrical Engineering	Alex Jones, Associate Professor
	Yiran Chen, Associate Professor
(Some centers for potential collaborations)	Gregory Reed, Professor
Potential centers or other units that will be affiliated: Center for Energy, Ridgeway Center, Center of National Preparedness, Center for Medical Innovation, John A. Jurenko Computer Architecture Laboratory, Center of Assistive Technologies, Medical Device Lab/Prototype Lab, RFID Center of Excellence, DBMI, UPMC	
Graduate School of Public and International Affairs	Louise Comfort, Professor
	Phil Williams, Professor
	Lisa Nelson, Associate Professor
Katz School of Business	Michael Donohoe, Clinical Associate Professor
School of Nursing	Rose Constantino, Associate Professor
SEI/CERT	**Sidney Faber, Adjunct Professor at SIS**
	Jonathan Spring, Adjunct Professor at SIS

NOTE: We note that while these three positions are long term goals, we expect these to be divided into two roles in the *short term* – one focusing on research and education and the other focusing on the remaining issues listed above.

- **Staff support**: The center will initially be supported by two administrative staff – one for internal administrative support and the other with expertise in outreach to industry and local and state government, providing primarily communications support (e.g., interfacing with external entities, developing communications materials, etc.). Two dedicated technical staff will oversee the operational aspect of the CyRes infrastructure.

CyRes Membership

Faculty members affiliated with the center are expected to represent a wide range of disciplines within Pitt. Listed in Table 1 is the initially identified individuals expected to be affiliated with the center, because of their research interest in CyRes relevant research or because they are already starting to collaborate in Cybersecurity research. Several of the listed members (in Bold) are already affiliated with LERSAIS. In addition to this, the center will extend our collaborative relationships with CMU's CyLab, SEI/CERT, NCFTA and UPMC, as well as other local partners.

We propose to extend the core cyber security expertise that will be affiliated to SIS-CS (new unit). The goal will be to ensure that the breadth of topic areas listed is covered in significant breadth/depth. While new hires will have primary expertise in cyber security, privacy, trust and resilience, they will have ancillary expertise related to a specific domain of priority for Pitt. While the CyRes research is the key expertise, we will seek the new hires that will uniquely add strengths towards these themes, as well as in filling other gaps that will assist in better collaboration with other domain specific areas.

These new hires will be structured along the lines of *Intelligent Systems Program* (ISP) at the Dietrich School of Arts and Sciences. ISP is a multidisciplinary program with faculty from many different units. Given even broader set of expertise needed and the interdisciplinary nature of CyRes field itself, we believe that such a program will be unique in this domain and will be able to further add to the research productive environment within the Center. The program would be able to award highly multidisciplinary degrees.

3.4 CyRes Fellows Program

We propose to create a Fellows program similar to that of Pitt's Center for the Philosophy of Science (CPS; see http://www.pitt.edu/~pittcntr/). The Fellows will be in the following categories: *Senior Visiting Fellow* (seniors in the field), *Visiting Fellow*, and *Postdoc Fellows*. CPS has been instrumental in garnering world-wide recognition for the History and Philosophy of Science program. We plan to structure the Fellows program similarly to propel CyRes towards similar world-wide recognition. The key goals are:

- Fostering broader, multidisciplinary collaboration with and among regional and international Cybersecurity experts. Special efforts will be made to bring well established visionaries as well as rising CyRes focused researchers to join us for a period of time (e.g., six months or one year). Fellows recruited will be from academia, industry or government research units.
- Identifying new directions in basic, transformative research and new opportunities for applied research. In particular, focus will be to explore the future research directions and establish plans for short-term and long-term collaborative activities (joint international proposals, large proposals such as SaTC, Expedition in Computing, etc.). Towards this, each year Fellows will be recruited around one or two CyRes themes. The goal will be to compose a holistic set of expertise around the identified themes. For instance, a theme could be Privacy; and expertise across the broader spectrum of privacy research - technical at different layers of IT environments, policy and regulations, Human factors, etc. - will be targeted.
- Providing CyRes student researchers an opportunity to experience working in a highly collaborative and agile research environment in presence of fellows so as to shape them for future research leadership.
- The Fellows will provide research seminars to CyRes researchers as well as other computing focused researchers within Pitt for exposure to broader research perspectives.
- The Fellows will also be engaged in conducting possibly team based research seminars for aspiring doctoral students on cutting edge issues.

- The Fellows will also work with CyRes researchers in planning International workshops and conferences in identified themes.

In summary, the Fellows program will be designed to significantly enhance the collaborative, multidisciplinary research setting and to foster a highly productive and research active environment.

3.5 CyRes PhD Fellowships

We strongly believe that a key factor in achieving the goals of the center is to have a constant pool of excellent PhD students deeply engaged in multidisciplinary research in the strategic subareas. The first five formative years are particularly very crucial. We seek to establish a 10-15 PhD fellowships to specifically generate significant momentum to push the center's agenda by attracting faculty from relevant domains of cybersecurity research. While we expect the CyRes faculty to generate significant funding to support PhD students with support from the center's seed funding, it is important to establish a core PhD Fellowship program to ensure that we maintain adequate level of research momentum. After the five years, we plan to rely on external support (Industry, Donors) to establish potential endowment funds to support the PhD fellowship program in future.

3.6 Annual CyRes Symposium

As a regular part of CyRes activities, we will organize *Annual CyRes Symposium* as follows:

- The Symposium will have two main days of activities focused on ongoing CyRes research with participation from all faculty, researchers and students affiliated with CyRes;
- Students will showcase their research in Poster and Demo sessions and/or presentation sessions.
- CyRes affiliated researchers (faculty, fellows, post-docs, etc.) will present their ongoing research activities and also float new ideas to explore; in particular, special sessions will be created to explore/discuss futuristic CyRes related issues/challenges;
- We will invite partners and distinguished people from public-private sectors who are potential funding sources and research partners. Significant efforts will be made to recruit new partners and invite/explore industry funding each year.
- The symposium will highlight distinguished invited talks, panel sessions and discussions on potential collaborative efforts.
- Awards and Recognition ceremony will be held to recognize donors, industry supporters, distinguished research achievements (e.g., CyRes Best Student/Faculty Research, etc.).
- Exploration of research fellowships and residency programs (e.g., for Industry researchers to visit CyRes and for CyRes researchers to visit Industry labs), student research internships, etc.
- CyRes Advisory Board meeting(s) will be held the day after the Symposium to explore new issues, recommendations, and opportunities. This would be leveraged to get feedback on ongoing activities.

An Industry/Gov Day. In addition to above, we plan to organize an **Industry/Government Day** to primarily focus on inviting Industry and Government researchers to talk about their research labs and to explore potential research collaborations. This will also be an opportunity for exploring research internships and CyRes fellows.

Cybersecurity Awareness Day. One day will be devoted to general community outreach – this includes research outreach to local industry and communities, and high school students and minority population. Participation of students (e.g., NSF SFS funded students) would be a key focus. At the same time, we will leverage CSSD's interest in generating Cybersecurity awareness for Pitt community and collaborate on that. One key goal will be to also disseminate research results through educational and awareness channels. Since October is the national ***Cybersecurity Awareness Month***, we believe that October would be an ideal time for this.

3.7 CyRes Research Infrastructure

A critical component for the center is the availability of a comprehensive research infrastructure that fosters holistic CyRes research. We envision building such a comprehensive research facility that will include the following components:

- ***Experimental Research Testbed***: This will provide support for experiments on foundational, systems/applications and networks, as well as domain specific cybersecurity testbeds (e.g., healthcare , SmartGrid, nuclear energy, etc.). These will include simulation environments and computing hardware and software components for CyRes relevant research. Various other units have specific capabilities (e.g., RFID lab, medical device lab, Centers of Energy and Nuclear Engineering, Center of National Preparedness, etc.) that we plan to leverage to build research computing infrastructure that extends and complements their capabilities so as to enable research in CyRes topics.

- ***Research Data Repository***: It is critical to have realistic simulated data, real data from networks/systems, test cases, etc., to support testing various hypotheses. The CyRes research infrastructures will be built to ensure extensive collection of such datasets. Collaborations will be leveraged to establish appropriately protected datasets from real world ICT environments (e.g., anonymized by ensuring appropriate level of utility). Easy connectivity and collaborations with other global units will be fostered to ensure one-stop availability of datasets that are critical for effective research. Initiatives to obtain such data have already begun with SEI/CERT and NCFTA.

- ***Software and Hardware Tools Repository***: The CyRes infrastructure will include extensive set of hardware and software tools that will be critical for supporting research experimentation. These include open source and commercial security tools relevant to various types of security research. One key emphasis will be to collect research prototypes – from both Pitt and outside - that will assist in research.

- ***Live Lab for Cyber Op & Forensics Research***: Cyber intelligence analysis, cyber operations and digital forensics are hands on and applied research areas. CyRes infrastructure will have physical space to accommodate real-time analytics, simulation and visualization capabilities and to support Cyber Attack-Defense (CA/D) simulations – such CA/D exercises will help guide further pragmatic research. Front end will include war room type of environment to experiment on real time testing of cyber attacks. Tools and techniques that support forensics and cyber operations will be extensively added – these will include testing Pitt's research prototypes, tools and techniques.

The goal of the CyRes infrastructure is to provide a comprehensive environment to enable all types of experimentation and validation work. The infrastructure will be developed along the lines of DETER (Cyber Defense Technology Experimental Research), PREDICT (Protected Repository for Defense of Infrastructure against Cyber Threats), and SWAMP (Software Assurance Marketplace) [15]. Facilities for

extensive cyber intelligence analysis and research, simulation and experimentation for various infrastructures are critically needed to address increasing cyber security concerns; Pitt's strong research presence in Nuclear, Energy, Healthcare (BodyNet/Internet of Medical Devices) Manufacturing, Transportation (Vehicular networks), etc., will be leveraged to build this infrastructure. We will pursue partnerships with industry research centers and local partners to create this rich research infrastructure.

We envision that two research staff will be needed to manage the research infrastructure and support CyRes faculty in using it for research. While responsible for overseeing the facility, they will also be engaged in research.

4. Effects on Other Units & Center Assessment

4.1 Effects on Other Units

Mutual Enhancements & Synergy: CyRes will bring together researchers in various domains to work with core CyRes researchers. Participation of domain specific experts in CyRes will significantly enhance cybersecurity research. At the same time, CyRes will catalyze the exploration of new efforts within the participating units/disciplines. These mutually enhancing activities will propel CyRes as well as domain specific research areas/centers to higher levels of recognition and success and, thus, will uniquely assist Pitt in achieving higher research excellence. For instance, CyRes collaboration with Nuclear cybersecurity will enhance research activities in both CyRes and Center of Nuclear Engineering – this will be mutually beneficial in terms of research visibility and impact for both units.

Efforts related to Center of Gravity in Computing/Informatics: The ongoing efforts to create the School of Computing and Information (SCI), which will be a *Center of Gravity* for computing and informatics at Pitt, have initially identified several signature research themes, listed below. While identifying these, cyber security has been recognized as a key *meta-theme* cross-cutting all the themes. CyRes thus will be able to play a central role, as part of the new SIS-CS unit, to catapult signature research themes selected to prominence.

Signature Research Themes identified so far are:

- Connected Life, Health and Medicine
- Modeling and Computational Tools for Scientific Discovery and Societal Good
- Computing at the Extremes
- Data Stewardship and Scientific Replicability
- Education for/by Computing
- Social Dynamics and Computing

Several CyRes sub-areas listed earlier cut across these themes. We plan to refine such sub-areas to closely align with the signature research themes once they are finalized. In particular, we see CyRes as the piece that will catapult the new SIS-CS unit as a *center of gravity for computing/information* at Pitt.

Cybersecurity Center of Excellence in Pittsburgh: Since last January, an effort to create a Cybersecurity Center of Excellence in Pittsburgh has been pursued at Pitt with the directive from the Chancellor based on a request from the PA Congressman Murphy. In the workshop Pitt organized to explore this initiative in Feb, 2015, about 40 local partners from academia, local government and industry participated with huge interest from all. It was clear that Pittsburgh can be a model *Cybersecurity City* in US with our active participation along with CyLab/CMU and SEI-CERT, as well as NCFTA, among others.

Formation of CyRes further strengthens our leadership role in creating a regional Cybercenter of Excellence.

4.2 Assessment of Accomplishments and Impact

The center's activities will be reviewed annually with respect to strategic goals and operational performance metrics. We will conduct a thorough review of the center's performance every year against the strategic plan. The center's performance will be assessed along the following three dimensions:

- **Research Productivity,** including:
  - New research collaborations enabled within the University
  - New funding / grants enabled by the center's activities
  - Sustained performance with respect to research output, as follows
    - Research publications by center members – with emphasis on both quality and quantity; fundamental as well as applied
    - Federally funded research (in dollar amounts)
    - Industry funding and partnerships
    - CyRes relevant MS/PhD theses
    - Participation in and sponsorship of research conferences and workshops highlighting multidisciplinary aspects of cyber security
    - External recognition of faculty, center, or associated programs
- Technology transfer through patents, software commercialization and entrepreneurial ventures, and open source tools and research datasets
    - The center will closely work with the commercialization infrastructure available at Pitt for this.
- **Research driven Education and Outreach,** including:
  - External assessment of the quality of center' program (s) or its affiliated programs
    - (e.g., CAE-R designation; Cyber Ops, Cyber Forensic programs)
  - Enrichment of cybersecurity curriculum through non-traditional integration across disciplines provided by CyREs research
    - New Cybersecurity degrees
    - Dual degree programs with Cybersecurity major/minor
    - Cybersecurity tracks with sub areas (e.g., the Security Assured Health Informatics subtrack)
  - Programs offered and students enrolled in undergraduate and graduate programs initiated and taught by the CyRes Faculty and affiliates in the SCI and collaborating schools.
  - Programs offered and students enrolled in outreach to or integration with K-12 schools, community colleges, local community organizations, etc.
    - We will leverage SIS's I^3 program, and SciTech collaboration, and other programs at Pitt for this.
  - Programs offered and professionals enrolled in for professional development aimed at practicing professionals and domain specific research.

Note that CyRes is essentially a research center, however, it is critical that educational activities are driven by research with a balance of both foundational and applied research. While educational programs will be conducted by other units CyRes will provide research-based guidance and oversight.

Such research-driven educational activities are also aligned with Pitt's goal of educational excellence.

- **Strength of Collaborations and Impact on Local/Global Communities,** including:
    - Establishment of new or strengthening of existing industry/government partnerships in research and education
    - Involvement in regional/global *CyRes* activities (e.g., within Pitt, in the greater Pittsburgh region, throughout the Commonwealth of Pennsylvania, etc.)
    - Success of the CyRes Fellows program.

5. Budgetary Considerations

Within five years, the Center will be self-sustaining through external funding and sponsored support from industry, and will generate a significant revenue stream for the University. Funding requested is intended to provide immediate administrative support from Pitt and to free existing faculty to pursue additional grants. Seed funding for new faculty both directly associated with the center and positioned within closely related academic units will be offset by new grants to these faculty and new students in tuition generating programs. **It is our belief that many of these positions can be filled by assuring that new hires to replace retiring faculty are targeted to be in line with cybersecurity.**

We overview various areas where funding will be needed and/or used based on the estimated budget of $21.40 Million in funding for the center over the five years. Table 1 below summarizes the distribution of the funds over various center related areas; it also shows the University funding (UNI) and the gradually increasing External funding (EXT) to meet the Center's projected budget of $21.40.

5.1 Center Start-up Funding

Startup funding will be needed immediately for following administrative and leadership functions:

- Staff support to assist the coordination team and the Center director in their day to day activities (meetings, communication; outreach activities, etc.)
- Staff to support the Center's website maintenance and communication activities (e.g., brochure, email communication, newsletters, support for report preparation)
- Technical staff for infrastructure management
- Compensation for faculty in leadership roles through reduction of teaching load and other research support (e.g., Center Director and Research Coordinator)

Estimated Budget: $5 M over FIVE years

Initially, the University would provide $1 Million for Center Start-up. Over the five years, costs would be transferred to external funding for staff support. Faculty administrative compensation would continue from the University, offset by additional soft money funding and overhead attributable to the center.

5.2 Small Grants Program

Seed funding to center-affiliated researchers to enhance cross-disciplinary collaboration. We envision a fund similar to existing Provost funding to provide small grants for teaching innovation and other such targeted efforts. We imagine 7-12 grants per cycle for three cycles over 5 years to support students and incidental expenses. The grants will foster multidisciplinary research and support novel individual explorations that aspire to create a pathway to new external funding
A few of these grants will be targeted to support ambitious, potentially high risk, high reward, projects (e.g., preparation for Expedition in Computing type proposals)

- Examples may include:
  1. Collaboration between faculty in IS/CS with Health/Nursing;
  2. Collaboration between IS/CS faculty from Centers of Energy/Nuclear Eng/Manufacturing/Quantum Info Processing, etc., or Cybersecurity Policy & Cybercrime
  3. Efforts to develop big data or quantum computing approaches to security

4. Collaboration between Social Network privacy and Cyberbullying research or Policy research

Estimated Budget: $3 M over FIVE years

We anticipate the total cost of this funding to be $3.0 million over 5 years. We expect these to support significant research initiatives in strategic areas so as to target external funding through federal sources and industry partnerships.

5.3 Cybersecurity Fellows Program

The Fellows Program will Support for 5-10 fellows per year and provide an ongoing series of signature workshops, conferences and seminars. For example, we currently have an active request to have 1 fellow supported by the Army War College. We anticipate being able to have additional fellows supported by industry either in support of a senior visiting industry researcher or industry support for an academic fellow focused on areas of interest to a particular organization or industry group.

Funds will be sought to have these fellowships sponsored by external funding. We anticipate ~100K/year for each fellow @ 5-10 fellows per year

Estimated Budget: $5 M over FIVE years

Of the $5M over five years, $2.75 is expected to come from UNI funding and the remaining will be generated through external sources, including corporate partnerships/support.

5.4 Seminar/Research-driven Educational Funds: These funds support the initial activities as follows:

a. Launch center-related seminars that emphasize multidisciplinary cybersecurity research and cyber operations;

Estimated Budget: $20K/Year (Total: $100K over five years)

b. Enhance research driven educational opportunities in cybersecurity

- Help create a multidisciplinary Cybersecurity Program (CsP) that offers PhD and research oriented Cybersecurity degrees.
- Help develop new cybersecurity sub tracks (both Professional MS and research oriented MS within CsP) in areas such as the following; importance will be given to innovation in teaching methodologies for Cybersecurity

Example tracks (primarily in Professional MS)

- SAIS track focusing on Legal/Cybercrime policy
- SAIS track with an economics/business/management component
- SAIS track with a health focus (currently under development with NSF funding)
- SAIS track with a sub focus on critical infrastructure protection (e.g., nuclear/manufacturing/transportation)
- Majors, minors, and dual degree programs could also be considered

Note: Core CyRes faculty will be part of CsP program. We would like to emphasize that CyRes faculty will help guide and design these programs and also explore research in

CyRes education/training. The funds will help the CyRes faculty members collaborate with others in exploring innovative, research-driven degree/training programs/modules.

Estimated Budget: (Total of ~$500K- 600K over 5 years)

- 2 MS/PhD students to help support the creation of new tracks or proposals for new tracks

c. **Annual CyRes Symposium & Travel to Funding related Information Session**: Travel to meet with potential funding sources and to explore local, regional and global partnerships

Estimated Budget: $60/year for five years (Total $300K) to support Annual CyRes Symposium and Travel (Corporate sponsorship will be sought/established within 5 year)

Estimated Budget: $1 M over FIVE years

Of the total budget, about 75% will be from UNI funding and rest will be generated through EXT sources. We will strive to go beyond the $1M projected funds for this through additional EXT funding.

5.5 **Faculty Hiring**: Over the initial five years period, the Center proposes that the University hire 8-12 new faculty members with about 60% or more focus on cyber security. Roughly half will be within the school with expertise in security, privacy, and related areas to establish a critical mass of faculty, as discussed earlier. We expect that additional new faculty will also be coming through new hires or existing faculty of other domain specific units.

It is anticipated that new faculty hires will come from vacancy opportunities, new cybersecurity faculty lines, and targeted hires for endowed positions. We envision two endowed chairs being hired in year 3. Opportunistic hires in affiliated departments will come as vacancies that can be targeted. All monies are shown as University funds which are offset by tuition dollars in associated programs and research overhead and direct support provided by new grants.

5.6 **CyRes PhD Fellowships**: Support for 10-15 PhD students/year for five years. We expect that CyRes researchers will immediately start generating funding research to support their PhD students – however, it will be important to jumpstart the multidisciplinary research in CyRes through initial PhD student support in the CsP.

Estimated Budget: $3 M over FIVE years

($2.1M will be through UNI funding and $0.9M will be EXT funding)

5.7 **CyRes Research facility**: While we expect to be able to manage with our current LERSAIS facility for another 2 years, the Center will need a larger physical facility that is easily accessible to a broader group of Pitt faculty. The facility would also provide office space for lead faculty members and staff, and include laboratory space (e.g., cyber forensic/operations labs, teaching/research labs, etc.), a large seminar room, collaboration space for affiliated students and faculty (e.g., student cyber security club, SFS room, space for PhD students). This facility will be designed with the needs of broader set of center's research activities, and will align with the needs of the Pittsburgh Cyber security center of excellence and Cyber Operational and Forensic activities.

We anticipate initial University support for equipping the Research and associated office space in

years 1 and 2, with ongoing funding and replenishment being funded out of external funding. The cost of outfitting the research space is estimated at about $2 million dollars, of which $1.2M is estimated to be coming out of the UNI funding.

Summary of Budget Distribution and Projected Revenue:

As mentioned earlier, Table 1 shows the funds from UNI and EXT sources that we estimate over five years to meet the projected need for the center for the first FIVE years. **The EXT total shown is minimum needed to achieve the center's projected level of five-year budget, given the University's support. However, our aim is to strive for more EXT funding so as to replace the UNI portions, wherever possible.** With regards to Table 1, we summarize the following key points:

- The University (UNI) will include support of $4.1M and $4.09 in years 1 and 2 respectively, to support the center formation and its activities. We anticipate EXT funding to kick in starting second year. The UNI portion will gradually decrease after year 2.
- ***Center Startup funds***: We anticipate distribution of funds for this to be evenly spread out in each year, with a total budget of $5M over 5 years.
- ***Small Grants Funding***: For this item, the main three seed funding cycles will be in years 2-4, with a smaller portion for year 1.
- ***CyRes Fellows***: We anticipate to gradually increase external funding for this item. In particular, we will explore corporate sponsorship to generate continuous funding to support it.
- ***Seminar/Research Educational Funds***: The initial funding will be used to initiate new efforts so that the center faculty can aggressively seek external funding to develop new educational programs and support research seminars (e.g., NSA CAE program, SFS program, etc.).
- ***Faculty Hiring***: Faculty hiring will be aggressively pursued. In year 1, we will strategically focus on hiring leading researchers who can provide immediate momentum and bring research funding. Subsequent hiring will be based on much longer term planning with focus on assistant professor level.
- ***PhD Students and Research Facility –*** For both these items, EXT funding sources will gradually become the primary source. We note that Small Grants and Faculty Hiring portions (total of $5.40M) are fully from UNI funding.

Center's Project Review: Table 2 shows the projected revenue that the Center will generate over the first five years because of the Center's resources and the affiliated faculty pool, with their curricular contributions and grants/funding related to cybersecurity education and research. For instance, with regards to tuition revenue, we can expect $25K/year/student from a cohort of about 40 cybersecurity students in year 1. Similarly, a huge potential opportunity exists for training and consulting revenue. For instance, in year 2, we can expect an average of $500/day/person of income; through the use of center resources, it is feasible to aim for 10 one-day courses with about 40 people/course.

Table 1. Projected Distribution of Funding between University (UNI) and the External (EXT) Funding sources													
All Numbers in $ Millions	Area Total	Year 1		Year 2		Year 3		Year 4		Year 5		Total/Area/Source	
Area		UNI	EXT	UNI	EXT	UNI	EXT	UNI	EXT	UNI	EXT	UNI	EXT
Center Start-up Costs	$5.00	$1.00	$0	$1.00	$0.10	$0.75	$0.30	$0.50	$0.50	$0.25	$0.60	$3.50	$1.50
Small Grants Funding	$3.00	$0.30	$0	$0.90	$0.00	$0.90	$0.00	$0.90	$0.00	$0.00	$0.00	$3.00	$0.00
CyRes Fellows	$5.00	$1.00	$0	$0.50	$0.25	$0.50	$0.73	$0.50	$0.25	$0.25	$1.00	$2.75	$2.23
Seminar/Research Educational Funds	$1.00	$0.20	$0	$0.15	$0.05	$0.20	$0.00	$0.10	$0.10	$0.10	$0.10	$0.75	$0.25
Faculty Hiring	$2.40	$0.60	$0	$0.60	$0.00	$0.72	$0.00	$0.24	$0.00	$0.24	$0.00	$2.40	$0.00
CyRes PhD Fellowships	$3.00	$0.60	$0	$0.54	$0.06	$0.45	$0.15	$0.30	$0.30	$0.21	$0.39	$2.10	$0.90
Research Facility	$2.00	$0.40	$0	$0.40	$0.20	$0.40	$0.20	$0.00	$0.20	$0.00	$0.20	$1.20	$0.80
Total/Year/Source		**$4.10**	**$0**	**$4.09**	**$0.66**	**$3.92**	**$1.38**	**$2.54**	**$1.35**	**$1.05**	**$2.29**		
Total by Year		**$4.10**		**$4.75**		**$5.30**		**$3.89**		**$3.34**			
Total University Cost												**$15.70**	
Total Externally Funded													**$5.68**
Grand Total (All Sources)													**$21.40**

Table 2. Estimated Center Related Revenue Generation over five years	In Millions					
	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Research Grants	$1.00	$1.30	$2.00	$2.30	$4.00	$10.60
Industry Collaboration	$0.00	$0.30	$0.40	$0.40	$0.50	$1.60
Tuition from Degree Programs	$0.50	$0.60	$0.80	$1.20	$1.40	$4.50
Training and Consulting	$0.00	$0.20	$0.40	$0.50	$0.50	$1.60
Total	$1.50	$2.40	$3.60	$4.40	$6.40	
Grand Total						**$18.30**

6. Comparison with Peers

There are several academic cybersecurity focused centers in US that are well established. While LERSAIS has existed for sometime the scope and size of research team has been significantly smaller to these other peers. Below we quickly highlight some centers that we aspire to compete and collaborate with, in no particular order.

- **CyLab at CMU** (https://www.cylab.cmu.edu/about/index.html): Considered as one of the best and largest Cybersecurity center in an academic institution in US, CyLab is a leader in this area. It lists more than 50 affiliated faculty members and over 100 graduate students from over six departments and schools. Various projects they currently focus on include: Trustworthy Computing Platforms & Devices, Next-Generation Secure & Available Networks Mobility, Security of Cyber-Physical Systems, Secure Home Computing Survivable Distributed Systems & Outsourced Services, and Privacy Protection. CyLab has significant funded security and privacy research and numerous industry partnerships. However, these projects do not typically combine technical and behavioral/ policy aspects of security and privacy. A subjective evaluation done by James Joshi roughly puts the size of CyLab researchers with Cybersecurity as the main focus at about 30 (to update) – rest will fall in the second-third circle in Figure 1. As part of CMU, SEI-CERT adds significantly to the strong cybersecurity research posture of CyLab.

  CyLab's strength is primarily on the technical excellence. A cursory comparison with Pitt's potential capabilities shows that Pitt has significantly more potential than CMU with regards to truly multidisciplinary and holistic research in this domain. In particular, various prominent engineering centers/programs (Energy, Nuclear, Manufacturing, RFID, Medical innovation, etc.), policy focused centers/programs (Ridgeway, CoNP, CoDM, etc.), healthcare (UPMC, HIM, Nursing, DBMI, etc.), and others (Business, Social sciences, Maths, Philosophy, etc.) provide ample opportunities to help create a more holistic CyRes research agenda.

  Important: While one approach is to develop CyRes to complement the excellence of CyLab, that approach will significantly limit Pitt's success, as follows: (i) it will create unnecessary dependence on CyLab's research agenda - this will have an effect of making Pitt's program second class; (ii) it will not make our research agenda as wholesome within Pitt as the opportunities present; (iii) collaboration across the institutional boundaries (between Pitt and CMU researchers) is tougher. We envision CyRes to be a competitor and collaborator with CyLab and other centers listed below, while ensuring our holistic and interdisciplinary research agenda. As a historic context, we had initial challenge in establishing the NSF SFS program, because of the fact that CMU already had well established SFS program. But we were able to overcome that, even though SFS program aims to evenly distribute its support across US.

- **GTISC at Georgia Tech** (**Georgia Tech Information Security Center**): It was established in 1998. It comprises of faculty, staff and students from multiple units across campus including the College of Computing, College of Engineering, College of Business, College of Liberal Arts, the Georgia Tech Office of Information Technology (OIT) and the Georgia Tech Research Institute (GTRI). Various cybersecurity research activities focus on secure communications hardware, prototyping, robotics & unmanned systems, systems/network security, threat modeling, and test & evaluation. GTISC lists about 36 faculty researchers. (Balaji Palanisamy's subjective evaluation estimates about 11-12 of them as primary and rest falling in second-third oval of Figure 1).

  There seems to be significant gap in research related to privacy aspects, end-user involvement, policy, healthcare and human factors at GTISC. And hence better set of opportunities for multidisciplinary research exist at Pitt, similar to what is mentioned above with regards to CyLab.

- The **Center for Education and Research in Information Assurance and Security** (CERIAS) at Purdue University (http://www.cerias.purdue.edu). It was established in 1998, evolving from COAST lab at Purdue. It lists affiliated faculty from six different colleges and 20+ departments across campus. CERIAS has been pursuing a huge number of projects that include Assured Identity and Privacy, Cryptology and Rights Management, End System Security, Human Centric Security, Network Security, Policy, Law and Management Prevention, Detection and Response, Security Awareness, Education, and Training. CERIAS lists about 81 Faculty affiliated with it. A subjective evaluation done by James Joshi indicates about 30-34 having cybersecurity/privacy as the primary focus, rest falling in the second-third circle in Figure 1.

  Similar arguments can be made, as above, with regards to unique strength that CyRes can have as compared to CERIAS. In particular, collaborative opportunities in the areas of Healthcare, RFID and medical devices, Policy/Legal, etc., quickly stand out.

- **The University of Maryland's Cybersecurity Center** (MC2) (http://www.cyber.umd.edu/about). MC2 lists about 40 affiliated faculty involved cybersecurity research areas such as: wireless and network security, secure software, cyber supply chain security, privacy of social networks, cybersecurity policy, cryptography, attacker behavioral analysis, health care IT, multimedia forensics, economics of cybersecurity, etc. The areas indicate broader coverage – however, Pitt presents broader opportunities through Policy, Healthcare and Engineering research centers. (No subjective evaluation on faculty size has been done yet)

- **UIUC Information Trust Institute ((**https://www.iti.illinois.edu/**)**: ITI research focuses on ways to making trustworthy information systems through modeling, measurement, and implementation based approaches. Their focus is on fundamental research/techniques towards building trustworthy systems, assessing their trustworthiness, and applying innovative techniques for critical applications, such as in aerospace systems, power systems, information systems, transportation systems, emergency response systems, and e-commerce and financial systems. Their current research is focused around following key themes: Power Grid, Health Information, Systems & Networking, Evaluation, and Data Science. ITI lists about 100 researchers affiliated to it . (No subjective evaluation on faculty size has been done yet). ITI represents cross-campus and cross-disciplinary initiative at UIUC focused on cybersecurity with participation from many departments and colleges. There is also significant effort on Science of Security area.

- **The Institute for Security, Technology, and Society (ISTS)** at Dartmouth College (http://www.ists.dartmouth.edu/about/). ISTS lists about 64 affiliated faculty members and emphasizes interdisciplinary research, education and outreach programs. They also emphasize areas such as Healthcare IT Security, Education Initiatives in Information Security and Privacy, and Network and Systems Security. Technical and behavioral issues, Policy side, CRI, are not clearly visible. (No subjective evaluation on faculty size is done yet).

- **JHU Information Security Institute** (ISI): ISI is the center for research and education in information security, assurance and privacy at JHU. Securing cyberspace and our national information infrastructure is more critical now than ever before, and it can be achieved only when the core technology, legal and policy issues are adequately addressed. They have good presence in secure networking, wireless, systems evaluation, medical privacy and electronic voting, among other areas (such as emergency health preparedness, bio-terrorism and national defense). The ISI lists 8 core faculty members and several other lecturers and staff members.

- **Stanford University**: Stanford has two key research centers focused on Cyber security – *Center for Internet and Society* in the Law School focused on cybersecurity laws, and *Computer Science Security Lab* which is focused primarily on the technical side of cybersecurity. CSSL has 11 CS faculty members with primary focus on cybersecurity. Stanford Cyber Initiative (https://cyber.stanford.edu/), with $15 million grant from HP in 2014, is focusing on studies of "cyber-social systems"; it is key place for a policy relevant research across various disciplines

- **UC Berkeley** – (https://www.eecs.berkeley.edu/Research/Areas/SEC/). Berkeley's Secure Research Lab has 6 primary and 18 secondary faculty members. Their research is focused on security, privacy, social implications of security, sensor web security, testbeds for security research (DETER, OceanStore, Wireless City Taipei), secure programming, human interfaces and security, identity and integrity, Network Security, Electronic voting, etc. Other centers within UC Berkley include Center for Evidence-based Security Research, Secure Computing Research for Users' Benefit (SCRUB), Team for Research in Ubiquitous Secure Technology (TRUST), etc. The new Center for Long-Term Cybersecurity (CLTC) was recently created with the help of HP support ($15 million; HP supported MIT, Stanford and UC-Berkley each with $15 million)

Compared to these Pitt has a broader set of highly recognized units that can add to the uniquely multidisciplinary CyRes environment, including: Healthcare, Energy, Nuclear, Manufacturing, International Policy and Social Sciences, Business, etc.

7. Proposed Implementation Plan

1. Year 1:
    a. Center basic infrastructure setup
        - Establish administrative setup (Directors, staff)
        - Center by-laws and detailing of the strategic plans
        - Membership
    b. Seed funding activities (every year henceforth)
    c. Explore partnerships/collaborations within and outside (to continue each year)
    d. Kick off CyRes Symposium
    e. Initiate CyRes Research Infrastructure design and planning
    f. Planning for recruitment of Faculty, CyRes PhD Fellowship, CyRes Fellowship program
2. Year 2:
    a. CyRes Research Infrastructure Development starts (or earlier than year 2)
    b. First Cohort of CyRes fellows
    c. Start faculty hiring
    d. Finalize administrative infrastructure
3. Year 3 & 5 onwards
    a. Continue Faculty hiring (until all lines filled)
    b. Seed funding
    c. Symposium & Fellowships continued
    d. Revisit priorities (sub-areas, strategic goals)
    e. Preliminary Review in year 3 on all aspects of the center for improvements
4. Year 5 onwards
    a. In additional to annual activities, do assessment/evaluation of the center

Significant concerted efforts will be made, as follows, towards the establishment of industry support and the success of getting competitive funding so as to sustain the center.

1. Monthly meetings of researchers to explore various funding opportunities and corporate partnerships,
2. Subareas focused meetings and/or reading groups will be organized to foster extensive interactions among the researchers to identify newer research problems and collaboration opportunities,
3. Arrange visits to and/or from industry and government on topics of high priorities to develop collaborative opportunities and to explore funding opportunities. Local industry partners will be aggressively pursued,
4. Special efforts will be made to motivate and bring onboard relevant faculty members from within Pitt to be affiliated to the center and/or to collaborate with the center faculty,
5. Special support infrastructure for helping center members in grant writing will be developed to help increase the chances of funding

References

[1] "5 huge cybersecurity breaches at companies you know" (http://fortune.com/2014/10/03/5-huge-cybersecurity-breaches-at-big-companies/)

[2] State of Cybersecurity: Implications for 2015 An ISACA and RSA Conference Survey (http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf)

[3] KPMG: "Health care and cyber security: Increasing Threats Require Increased Capabilities (http://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf)

[4] Obama's 2016 Budget Proposal Allots $5.5B for DoD Cyber Operations (http://www.executivegov.com/2015/03/obamas-2016-budget-proposal-allots-5-5b-for-dod-cyber-operations/)

[5] Cybersecurity gets big boost in 2016 budget (https://gcn.com/articles/2015/02/03/budget-cybersecurity.aspx)

[6] James F. Kurose, PhD. "The Expanding Cyber Threat," Before the Subcommittee on Research and technology, Jan 27, 2015

[7] Mandiant Report: "APT1: Exposing One of China's Cyber Espionage Units", 2011 (http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)

[8] Ponenom Report

[9] J. Healy, N. Pollard, B. Woods, "The Healthcare Internet of Things; Rewards and Risks" Atlantic Council (http://www.mcafee.com/us/resources/reports/rp-healthcare-iot-rewards-risks.pdf)

[10] Forbes article: "America's Critical Infrastructure Is Vulnerable To Cyber Attacks" (http://www.forbes.com/sites/realspin/2014/11/11/americas-critical-infrastructure-is-vulnerable-to-cyber-attacks/)

[11] "Report on Cybersecurity and Critical Infrastructure in the Americas" in Trend Micro

[12] "Ongoing Sophisticated Malware Campaign Compromising ICS" Black Energy Malware", (https://industrialcontrolsecurityusa.com/ongoing-sophisticated-malware-campaign-compromising-ics-black-energy-malware/)

[13] "Report finds many nuclear power plant systems "insecure by design" (http://arstechnica.com/security/2015/10/report-finds-many-nuclear-power-plant-systems-insecure-by-design/)

[14] James Kurose

[15] "Cybersecurity to Grow by 121% in the Next Five Years," (https://beta.finance.yahoo.com/news/cybersecurity-grow-121-next-five-220439932.html?ltr=1)

[16] Cyber crime costs global economy $445 billion a year: report (http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609#4WRVSy41uEdzIWFl.97)

[17] "CYBER ESPIONAGE AND THE THEFT OF U.S. INTELLECTUAL PROPERTY AND TECHNOLOGY" HEARING BEFORE THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS OF THE COMMITTEE ON ENERGY AND COMMERCE HOUSE OF REPRESENTATIVES ONE HUNDRED THIRTEENTH CONGRESS (http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm)

[18] "INTERNET SECURITY THREAT REPORT 2014", Symantec (http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf)

[19] Douglas Maughan, David Balenson, Ulf Lindqvist, Zachary Tudor, "Government-Funded R&D to Drive Cybersecurity Technologies", IT Professional, vol.17, no. 4, pp. 62-65, July-Aug. 2015, doi:10.1109/MITP.2015.70

[20] https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/

[21] http://www.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/

Appendix A: Grants of Core SIS LERSAIS Faculty

- **(Double check other relevant grants)**

- **James Joshi** (PI), P. Krishnamurthy, and D. Tipper, NSA CAE Cybersecurity Grant, "Towards Insider Threat Assessment and Mitigation," 2014 – 2015, Amount: $264,553
- **Adam J. Lee** (**PI**), "CAREER: UCPriv: User-Centric Privacy Management," National Science Foundation Award No. CNS–1253204 09/2013–08/2018; $545,623 to Pitt
- **James Joshi (PI),** Konstantinos Pelechrinis, Balaji Palanisamy, Bambang Parmanto, Prashant Krishnamurthy, "*A Curriculum for Security Assured Health Informatics*," NSF-DGE Award (2014 - 2017); Award Amount: $897,055.00 [Senior Personnel: Michael Spring, David Tipper, Leming Zhao]
- **Adam J. Lee** (PI), "TWC: Medium: Collaborative: Foundations of Application-Sensitive Access Control Evaluation," National Science Foundation Award No. CNS–1228697 09/2012–08/2015; $254,525 to Pitt of $1,109,562 total; Joint with Timothy Hinrichs and Lenore Zuck (University of Illinois at Chicago), and Von Welch (Indiana University at Bloomington)
- **M. B. Spring (PI)**, Martin Weiss, James Joshi, P. Krishnamurthy, D. Tipper, "*Standards: People, Process, Products and Productivity Focus on Information Technology Standards*," NIST Program, Amount: $99,535, Period: 2013-20014 (***Has cybersecurity components***)
- **Adam J. Lee** (**PI**), "TC: Medium: Collaborative Research: Towards Formal, Risk-Aware Authorization," National Science Foundation Award No. CNS-0964295, 06/2010–05/2014; $329,274 to Pitt of $1,094,022 total; Joint with David K.Y. Yau (Purdue) and Marianne Winslett (Univ. Illinois at Urbana-Champaign)
- **J. Joshi (PI)**, "*DiCoTraM*: *Towards a Distributed Collaborative Traffic Monitoring System*," Amount: $54,034; Period: 2012-2013 CISCO.
- **Adam J. Lee** (PI), "TC: Small: Collaborative Research: Improved Privacy Through Exposure Control," National Science Foundation Award No. CNS-1017229, 09/2010–08/2013; $149,859 to Pitt of $419,859 total Joint with Apu Kapadia (Indiana University at Bloomington)

- **James Joshi (PI),** P. Krishnamurthy, M. Spring, D. Tipper, "*A Scholarship Program for Security Assured Information Systems Track*," **National Science Foundation CyberCorp (SFS) Program**, 8/11/11 – 8/11/14, $1,290,000.
- **Daniel Mosse** (PI) and Adam J. Lee (Co-PI), "Distributed, Verified, and Trustworthy Protocols for Mobile Spacecraft Coalitions," DARPA Award No. NNA11AB36C, 05/2011–11/2011; $201,158
- Leming Zhao (PI), Bambang Parmanto, Qi Mi, Mervat Abdelhak, **James Joshi (Co-PI),** "*CPATH-1: Health Computing: Integrating Computational Thinking into Health Science Education," NSF CPATH, Amount: $104,537.00, Period: 2007-2009.* ***(Joshi's part was Information Security)***
- **Adam J. Lee** (PI), "TC: Small: Collaborative Research: Towards a Dynamic and Composable Model of Trust," National Science Foundation Award No. CCF-0916015, 09/2009–08/2012; $231,248 to Pitt of $465,582 total; Joint with Ting Yu (North Carolina State University)
- **J. Joshi (PI)**, "*A Trust-based Access Control Management Framework for Secure Information Sharing and Multimedia Workflows in Heterogeneous Environments,"* **National Science Foundation CAREER program,** Amount: $416,419.00; Period: 2006-2011
- **J. Joshi (PI)**, P. Krishnamurthy, M. Spring, D. Tipper, "*A Scholarship Program for Security Assured Information Systems Track*," **National Science Foundation CyberCorp (SFS) Program**, 8/11/06 – 8/11/10, $1,055,553.
- **K. Pelechrinis**, "*Building and Maintaining Trust in Wireless Networks*," Central Research Development Fund from University of Pittsburgh, $15,750, 7/1/2011-6/30/2013.
- P. Mohapatra, S. F. Wu, K. Levitt, J.J.Garcia-Luna-Aceves, T. La Porta, G. Cao, S. Krishnamurthy, M. Faloutsos, **P. Krishnamurthy, D. Tipper**, S. Kasera, L. Swindlehurst, "*ARSENAL*: *A cross layer Architecture for Secure resilient tactical mobile ad hoc networks*," **Army Research Office MURI Grant** , 7/01/07 – 11/30/13, $6,500,000 (David Tipper was PI of University of Pittsburgh portion $715,000).
- **P. Krishnamurthy (PI)** : Collaborative Research: NeTS: WN: *Coping with Jamming Attacks in Ad hoc* / Mesh *Networks* ($149,998.00, 2007 – 2010)
- **D. Tipper** (**PI),** J. Joshi, and P. Krishnamurthy, "*Dynamic Data Driven Defense Mechanisms for Cybersecurity*," **National Science Foundation CSR-SGER Program**, 8/1/07-7/30/09, $104,000.
- K. Trivedi, D. Medhi and **D. Tipper (PI)**, "*MiMANSaS*: *Metrics, Models and Analysis of Network Security and Survivability*" **National Science Foundation CT-ER Program**, 09/01/08 – 08/30/10, $169,834
- **James B. D. Joshi (PI)**, P. Krishnamurthy, D. W. Tipper, M. B. Spring. "*Capacity Building* (*Research + Equipments*) *and IRMC Partnership,"* DoD IA Scholarship Program, ~$55,000 (Capacity Building only), 2006
- **James B. D. Joshi (PI)**, P. Krishnamurthy, D. W. Tipper, M. B. Spring. *Program Partnership with the Information Resource Management College* (IRMC) *of the National Defense,* DoD IA Scholarship Program, $273,660, (approved overall budget); in 2005
- **James B. D. Joshi (PI)**, P. Krishnamurthy, D. W. Tipper, M. B. Spring, CIAG CISCO Equipment Grant WINNERS, *A Proposal for Cisco CIAG Equipment Grant,"* - ~$130,000, 2005
- **M. B. Spring (PI),** P. Krishnamurthy, D. Tipper, J. Joshi, *"A Curriculum in Security Assured Information Systems,"* NSF Federal Cyber Service, $283,640; Period: 2004-2006
- **James B. D. Joshi (PI)**, *An Adaptive Framework for Security-Assured Survivable Information Systems;* University of Pittsburgh CRDF, Amount: $19,988; Year: 2004-2006
- **M. B. Spring** "*Role Assured Publicly Accessible Information* (RAPAI)" - $25,000, 2004; (Dean's Entrepreneurial Initiatives)

- **J. B. D. Joshi, P. Krishnamurthy, D. W. Tipper, M. B. Spring** *"Laboratory Of Education And Research On Security Assured Information Systems* (LERSAIS)," - $12,000, 2004, (Dean's Entrepreneurial Initiatives)
- **P. Krishnamurthy,** D. W. Tipper, J. Kabara "Survivable And Secure Wireless Information Architecture," - $432,076 08/01 - 08/03 (Sponsor: National Institute of Standards (NIST) Critical Infrastructure Protection Grant)
- **D. Tipper** and T. Dahlberg (Sponsor: NSF ANIR Program), "Design And Restoration Techniques For Fault Tolerant Wireless Access Networks," - $300,000 9/15/00 - 9/15/03
- P. Krishnamurthy and J.F. Kabara (Pitt CRDF), security architecture for wireless residential networks - $13,230 1999
- D. Medhi and **D. Tipper** (Sponsor: Defense Advanced Research Projects Agency, (DARPA)), "Self-Configuring Multi-Networks For Information Systems Survivability" - $1,251,241 7/1/97 - 6/30/00
- **D. Tipper** and D. Medhi (Sponsor: National Science Foundation CCR Program), "Network Design And Traffic Recovery Procedures For Survivable Wide Area Networks" - $274,097 FOR FACULTY AND STUDENT SUPPORT 8/95 - 6/98
- Supplemented by "NSF Research Experience for Undergraduates," Fall 96, $5,000 for student support.

Appendix B: Summary of Security Education at LERSAIS

- Designated as CAE and CAE-R jointly by NSA/DHS till 2021
- Offering Security Assured Information Systems (SAIS) track since 2004
    - In MS IS and MST degree programs
    - 24 Credit CAS in SAIS
- 15 Credit Post-bac and Post-graduate CAS
    - Since 2014
    - Online offering started in Spring, 2015
- NSF Supported Scholarship for Service Program since 2006
- DoD IASP program for several years (Lab capacity development, short projects, scholarship support)

Appendix C

Examples of some General Funding sources and some specific calls this year

- National Science Foundation (SaTC, Core Programs, Expedition in Computing, CyberCorps/SFS, Smart-health & Well-being, etc.)
- NSA/DHS –
    - CAE Cyber security program
    - Broad Agency Announcement Solicitation HSHQDC-16-R-B0003; Project: Application Security Threat Attack Modeling (ASTAM)
    - Broad Agency Announcement Solicitation HSHQDC-16-R-B0002; Project: Static Tool Analysis Modernization Project (STAMP)
    -
- Office of Naval Research (ONR)

    - Real-Time Full Spectrum Cyber Science & Technology (Dept of Navy)
- Department of Army: Innovative Cross-Domain Cyber Reactive Information Sharing (ICCyRIS) (https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=0fd8b2649243b45f3d38f326499ca14d)
- Department of the Air Force:
    - Innovative Cross-Domain Cyber Reactive Information Sharing (ICCyRIS): https://www.fbo.gov/index?s=opportunity&mode=form&id=b0e6dc11fb3ebb703e286c44dcc740d8&tab=core&_cview=1
    - Next Generation Intelligence Collection and Analyses: https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA-AFRL-RIK-2015-0006/listing.html
    - Advanced Cyber, SIGINT and Personal Communications Collection and Exploitation: https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA-AFRL-RIK-2015-0022/listing.html
    - Multi-INT Enhanced Exploitation and Analysis Tools (E2AT): https://www.fbo.gov/spg/USAF/AFMC/AFRLRRS/BAA-RIK-12-13/listing.html
- Naval Air Systems Command, "Broad Agency Announcement (BAA) for Resilient Cyber Warfare Capabilities," : https://www.fbo.gov/spg/DON/NAVAIR/N68335/N68335-15-R-0179/listing.html
- Office of Naval Research: Naval Supply Systems Command: Multi-INT Research Initiatives at The Naval Postgraduate School Grant: http://www.grants.gov/web/grants/view-opportunity.html?oppId=279229