Applications of Distributed Socio-technical Synthetic Intelligent (SI) Systems Using Hybrid "Compensating Controls" Architectures

Barbara Endicott-Popovsky(✉)

University of Washington CIAC, Seattle, WA, USA
endicott@uw.edu

Abstract. At least weekly we hear about significant data breaches or cyber-attacks that threaten the financial health and privacy of millions of online users, or about attacks by nation states or terrorist groups with a political or propagandistic agenda. How did we get here? How did our online interconnectedness that has created so many benefits, resulted in so many challenges? We're living through digital transformation that's challenging how we think about the world. We are clinging to mental models from the physical world and the industrial age that no longer work. What we need are new mental models and a recognition that technology alone does not fix the problem. It's the humans in the system that require rules for operating online that need to be vigorously addressed. Here is a case for new hybrid architectures that combine both the rules and tools for operating online. Some way to institute neighborhood watch with compensating controls that bridge the gap between humans and current technologies.

Keywords: Cybersecurity · Information Assurance · Synthetic intelligence
Compensating controls

1 Introduction

To provide context to this discussion, four major concepts about cybersecurity drive our work and our views.

1.1 In Cyberspace, EVERYONE Is Our Neighbor

Living in the United States, we have had the luxury of two oceans on either side, left and right, with two 'soft' countries above and below that are basically cooperative and 'like us.' This may have inured us to what we have done to ourselves online by becoming virtual next door neighbors with all of our 'friends' around the world.

Now we are side-by-side with cultures and countries radically different from our own, with very different world views about intellectual property (IP), freedom of speech, ethics, etc.[1] Why do we expect them to behave like us? Why should they? This requires new deeper insights into how other societies function and how we cooperate with them online.

[1] Read The Lure [1].

P. Zaphiris and A. Ioannou (Eds.): LCT 2018, LNCS 10925, pp. 276–285, 2018.
https://doi.org/10.1007/978-3-319-91152-6_22

Further, relationships between the military, government, industry, and citizens in the United States are being rethought in light of sharing the same networks. Most US critical infrastructure is non-federal, which means states, tribes, and municipalities, as well as private industry, fend for themselves when attacked. A new type of cross sector collaboration, proposed in US Congressional bill HR 3712, the Major General Tim Lowenberg National Guard Cyber Defenders Act, establishes National Guard Cyber Civil Support Teams in every state. Cyber CSTs would serve as first-responders to incidents under the direction of governors and the state adjutant general, building a trusted link between states, critical infrastructure providers, and federal government.

The Center for Information Assurance and Cybersecurity has pioneered cross sector collaborations (Fig. 1) throughout its history, studying the challenges of working interconnectedly. Finding shared missions is key to success since each sector has its own individual mission—industry/profitability; government and military/safety and security. Safety and security of citizenry is an understandable shared mission that critical infrastructure can embrace. We will discuss an example of implementing this idea later in the paper.

1.2 Cybersecurity Involves Rules and Tools

Although rooted in technology, there is no firewall for stupidity! Cybersecurity in organizations also depends on the elements that manage the human nodes in the network—the policies and processes at all levels, communication, and problem-solving approaches. We call these the ‘rules’ component of the rules and tools controls required to secure systems, as described in Fig. 2.

Reading Fig. 2, the Goals of an organization, influenced by budgetary constraints, applicable laws and regulations and standards, result in appropriately aligned organizational policies, which are implemented in controls: procedures that regulate human behavior and technologies. Information about these controls is disseminated to every human in the total system through effective security awareness training. This results in a secure organizational environment which must be managed and audited regularly for compliance, since the adversaries arrayed against systems are in an ‘arms race’ with defenders [2]. Those managing cybersecurity in organizations should anticipate a rapidly changing technical and legal landscape which will require continuous change.

This model was synthesized through data collection of the activities of Chief Information Security Officers (CISO) in the Northwest and affinitized to create the chart in Fig. 2. What started as a long laundry list of tasks was grouped in the elements that require management in a cyber secure organization. It’s much easier to keep track of these few elements than a long list of tasks and it has provided the foundation for CIAC’s educational programs which are to CISOs what the MBA is to CEOs. The programs provide an overview of the cybersecurity responsibilities allowing students to find their career pathway as the pathways proliferate discussed in Sect. 1.4 below.

1.3 Not Enough Talent

Compounding cybersecurity problems, there is a systemic shortage of well-trained talent (and of qualified teachers). The National Institute of Standards (NIST) has

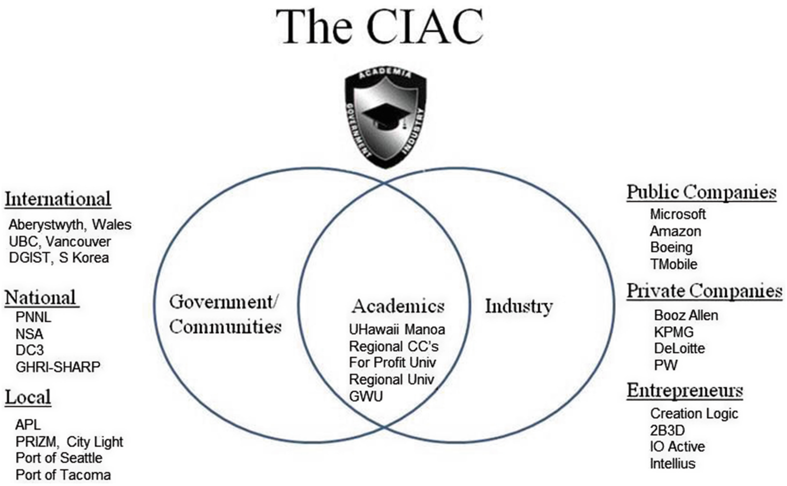


Fig. 1. CIAC Cross sector collaborations

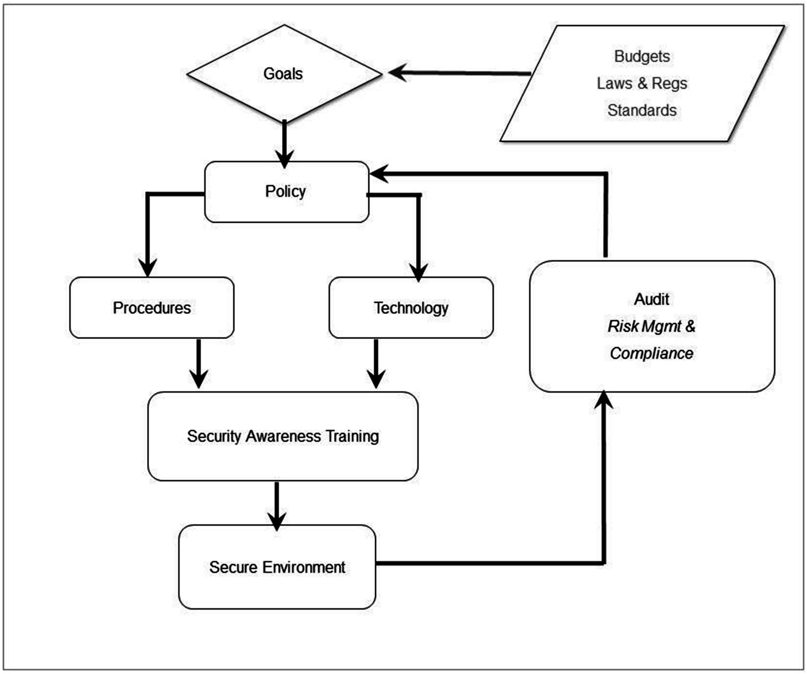


Fig. 2. Operational environment for managing cybersecurity

created the National Initiative for Cybersecurity Education (NICE) to address both insufficient supplies of cybersecurity talent and the length of time that it takes to develop 'breach-ready' effective cyber responders. To gain an understanding of the enormity of the deficit, NIST, in partnership with Burning Glass—a consulting firm exploring talent shortages, have created cyberseek.org that tracks unfilled jobs in cybersecurity by US county and by type of job (Fig. 3).

Double the reported unfilled positions to add deficits worldwide.

1.4 Cybersecurity Is Becoming a Profession and Developing Specialties

Complicating the search for talent, there are now 36 separate career paths identified within the cybersecurity field. Each has its own tasks and associated knowledge, skills and abilities. To organize this complexity for employers and job candidates, employment and education standards are emerging that employers can rely upon when pursuing talent and students can apply to their own career preparation efforts.

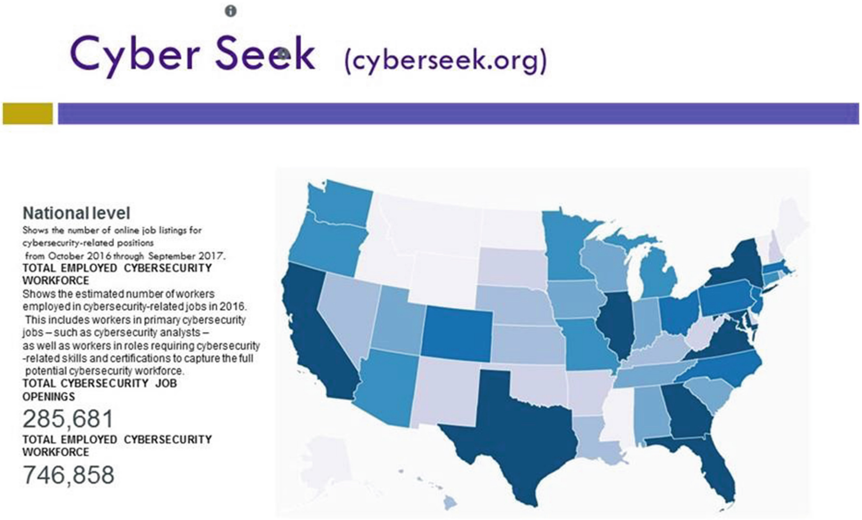
Further, the field is professionalizing, like the medical field, with behavior norms, codes of ethics, progression through internships and cooperative learning arrangements supported by requirements for certain types of certifications. Changes are occurring rapidly. The NICE initiative changes as the field changes and can be tracked on their website Fig. 4).

These four foundational ideas focus on the human in the cybersecurity system, the weakest link. While much research in this field focuses on technical controls, little has been done to study what the authors call ‘compensating controls,’ alternative controls that satisfy security requirements that cannot be implemented in traditional technical control systems at the present time. These circumstances beg for engineering augmented cognition for these distributed socio-technical synthetic intelligent (SI) systems through hybrid architectures that combine augmented cognition and traditional technical controls. This will require new ways of thinking about cybersecurity and a change in our traditional mental models that describe cybersecurity within today’s systems. Before providing examples of ways of thinking that could be modified, we should look at how we got to this point.

2 Cyberattacks: How Did We Get Here?

At least weekly we hear about significant data breaches or cyberattacks that threaten the financial health and privacy of millions of online users, or about attacks by nation states or terrorist groups with a political or propagandistic agenda. To the citizen observer, it must appear that those responsible for managing networks are helpless to do anything about rising online crime and threats. To a certain extent that assumption is true. We will never have 100% secure systems as long as we have humans in the system. Today, technologies alone won’t ‘fix’ our cybersecurity vulnerabilities. Users do assume a certain amount of risk online whether they realize that, or not. This idea shatters a comfortable sense of security developed in first world nations over decades of experiencing reliable infrastructure. It’s no wonder the public is disturbed by the news of cyber threats to infrastructure connected online. There is no cyber fire department to call if things don’t work.

How did we get here? How did our online interconnectedness that has created so many benefits, resulted in so many challenges? Have we been so enamored of creating



Cyber Seek (cyberseek.org)

National level

Shows the number of online job listings for cybersecurity-related positions from October 2016 through September 2017.

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

Shows the estimated number of workers employed in cybersecurity-related jobs in 2016. This includes workers in primary cybersecurity jobs – such as cybersecurity analysts – as well as workers in roles requiring cybersecurity-related skills and certifications to capture the full potential cybersecurity workforce.

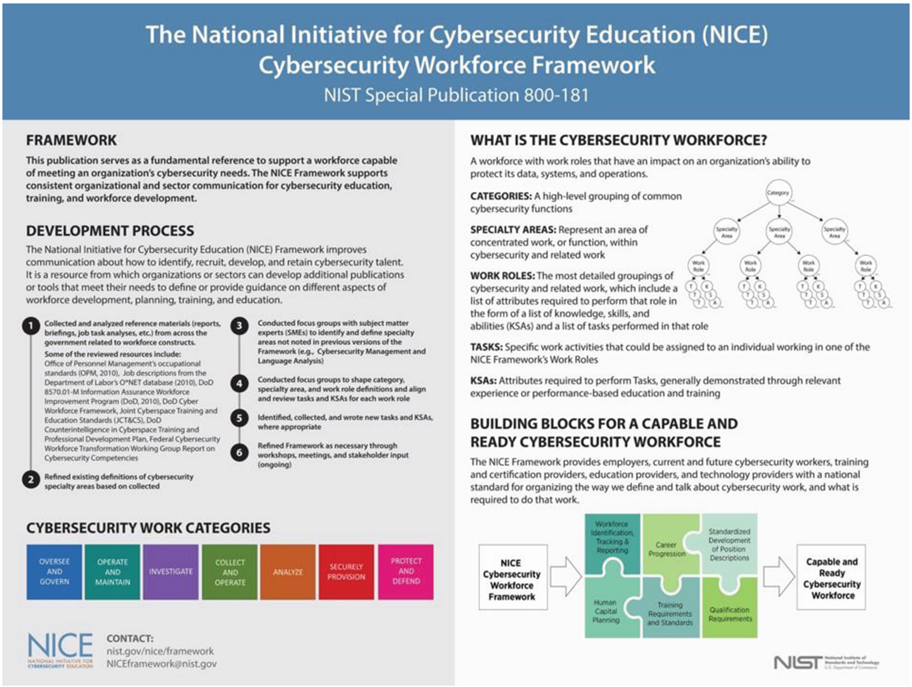
TOTAL CYBERSECURITY JOB OPENINGS

285,681

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

746,858

Fig. 3. Cyber seek for tracking unfilled US cybersecurity jobs



The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

NIST Special Publication 800-181

FRAMEWORK

This publication serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. The NICE Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development.

DEVELOPMENT PROCESS

The National Initiative for Cybersecurity Education (NICE) Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

1 **Collected and analyzed reference materials (reports, briefings, job task analyses, etc.) from across the government related to workforce constructs.**
Some of the reviewed resources include:
Office of Personnel Management's occupational standards (OPM, 2010), Job descriptions from the Department of Labor's O*NET database (2010), DoD 8570.01-M Information Assurance Workforce Improvement Program (DoD, 2010), DoD Cyber Workforce Framework, Joint Cyberspace Training and Education Standards (JCT&CS), DoD Counterintelligence in Cyberspace Training and Professional Development Plan, Federal Cybersecurity Workforce Transformation Working Group Report on Cybersecurity Competencies

2 **Refined existing definitions of cybersecurity specialty areas based on collected**

3 **Conducted focus groups with subject matter experts (SMEs) to identify and define specialty areas not noted in previous versions of the Framework (e.g., Cybersecurity Management and Language Analysis)**

4 **Conducted focus groups to shape category, specialty area, and work role definitions and align and review tasks and KSAs for each work role**

5 **Identified, collected, and wrote new tasks and KSAs, where appropriate**

6 **Refined Framework as necessary through workshops, meetings, and stakeholder input (ongoing)**

CYBERSECURITY WORK CATEGORIES

OVERSEE AND GOVERN | OPERATE AND MAINTAIN | INVESTIGATE | COLLECT AND OPERATE | ANALYZE | SECURELY PROVISION | PROTECT AND DEFEND

NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

CONTACT:
nist.gov/nice/framework
NICEframework@nist.gov

WHAT IS THE CYBERSECURITY WORKFORCE?

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.

CATEGORIES: A high-level grouping of common cybersecurity functions

SPECIALTY AREAS: Represent an area of concentrated work, or function, within cybersecurity and related work

WORK ROLES: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role

TASKS: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

BUILDING BLOCKS FOR A CAPABLE AND READY CYBERSECURITY WORKFORCE

The NICE Framework provides employers, current and future cybersecurity workers, training and certification providers, education providers, and technology providers with a national standard for organizing the way we define and talk about cybersecurity work, and what is required to do that work.

NICE Cybersecurity Workforce Framework
Workforce Identification, Tracking & Reporting
Career Progression
Standardized Development of Position Descriptions
Human Capital Planning
Training Requirements and Standards
Qualification Requirements
Capable and Ready Cybersecurity Workforce
NIST National Institute of Standards and Technology U.S. Department of Commerce

Fig. 4. NICE framework standardizing cybersecurity workforce specialties (NICE Workforce Framework: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework)

the next new digital device or online service that we haven't taken time to consider the unintended consequences that we've introduced into our lives [3]?

We're living through digital transformation that's challenging how we think about the world and that's breaching the silos that once organized our lives and our thinking [4]. We have been clinging to mental models from the physical world and the Industrial Age that blind us to the changes around us. The embrasure of technology is moving so fast, it's difficult to keep up with the unintended consequences of what this has done to our daily reality and how society functions.

In one sense, we are rapidly smashing our Industrial Age mental models where organizations are structured in hierarchies, knowledge is structured by discipline, our work is in discrete silos—departments and sectors: military, government, industry, academia—replacing it with an interconnectedness that, as a by-product, also enables online fraud, online voting scams, illegal downloads, and continuing threats to network security.

But who saw this coming? Like Mickey Mouse as the Sorceror's Apprentice in Fantasia, we have assumed the wizard's powers without anticipating the risks [5, 6]! What was meant for good has ushered in unexpected problems. The internet has brought convenience, savings, and productivity, but it also has created troubling dislocations that we didn't anticipate that we are beginning to face now as a society.

3 New Mental Models Needed

New ways of thinking about the world are needed as the digital transformation continues. For example, the Industrial Age organized work into discipline silos (legal, engineering, human resources, manufacturing) and assembly lines dividing up work steps for mass production. What we need is a systems approach to thinking through what new models for social interaction are needed for a more digitally interconnected world [7]. A few new concepts are suggested below.

(1) Cross Sector Collaboration: Public Private Partnerships

US citizens are accustomed to calling 911 for emergencies of all kinds, and similar emergency response is offered in other countries, but who do you call in the event of a major cyber outage? In the US, the Department of Defense (DoD) is prepared to defend its own networks to support their missions, but who will step in on the civilian and private sector sides to restore power, to assist with maintaining communities? This vacuum is a national security vulnerability.

We need a new way to think about public/private partnerships. One state[2] has benefited from a National Guard[3] whose leadership, coming from the tech industry in that state, has created cyber civil support teams that assist government agencies and utilities to assess their vulnerabilities in advance of a major cyber event and respond in

[2] Washington State National Guard are leaders in this approach.

[3] The National Guard of the United States, is part of the reserve components of the US Armed Forces, composed of units of each state and the territories, a total of 54 separate organizations. Units are under the dual control of the state and federal governments.

the case of a major cyber disaster. Working across civilian and military boundaries is not easy, given legal authorities issues; however, their lessons learned about crossing authorities in nanoseconds is preparing private sector infrastructure for a major cyber event and could be disseminated across the US and other countries, for maximum preparedness.

Critical infrastructure private sector partners have an opportunity to leverage the work of the National Guard to increase their surge capacity [8]. One contribution from such a public/private partnership would be the coordination of credentialing, training, and funding of cyber disaster command centers.[4]

Public and private sectors have two very different missions: the public sector mission is to protect the homeland, and the private sector innovates and maintains profitability for stakeholders. Blending missions between the two is not an easy task, but the cost of not integrating resources significantly outweighs the benefits. One important mission nexus they both can accept is the need for providing life safety. Profitability becomes secondary to public safety.

(2) Cyberwar: Grasping a New Case of Mutually Assured Destruction

The US has had the luxury of two oceans on either side, with two ‘soft’ countries above and below inuring citizens to the unintended consequences of becoming virtual next door neighbors with countries with active cyber warfare programs. (See earlier discussion.) At some point we can anticipate the need for (1) the equivalent of Soviet era ‘red phones’ to ensure we don’t misread each other’s online intentions and (2) the equivalent of ‘nuclear disarmament’ talks to define the rules of acceptable online behaviors for civil societies.

Cyberwarfare can be as deadly as nuclear war and could conceivably result in mutually assured destruction. (Think of failures in the transportation industry or hospitals shutting down or food being massively poisoned.) At the moment, enforcement of appropriate online behavior for individuals is challenging, but you are seeing the beginnings of some controls on speech.[5] As of yet, it doesn’t appear that nation state users have an appetite to lay down agreed-to standards for warfare, although you are seeing the beginnings of the discussion [9].

3.1 Tragedy of the Commons

We’ve just described an Information Age case of the ‘Tragedy of the Commons,’ in which a shared-resource, the internet, is accessed by users who act independently according to their own self-interest, behaving contrary to the common good, thus spoiling that resource for all. This argues for agreed-to behavior standards, but there would need to be a means of enforcement. This has not proven easy in the case of

[4] H.R. 3712 – Major General Tim Lowenberg National Guard Cyber Defenders Act proposes funding for this activity within the State of Washington.

[5] The idea of harmful speech is not new. For example, it is unlawful in the US to cry “fire” in a crowded venue if no fire is observed. Today, we are seeing various social media giants wrestling with the idea of free vs. harmful speech in an effort to regulate it. This has generated controversy, but it also has begun the discussion.

individuals and in the case of nation states there seems to be no appetite. We are left with either waiting for a catastrophic failure before a solution is developed, or with instituting thoughtful interim behaviors by all users, during this interesting period, while we shed Industrial Age mental models for something as yet to be developed.

4 Talent Deficit

Unfortunately, there is a huge deficit in talent prepared to handle these cyber problems. This lack of talent is keenly felt across all sectors of the US economy—industry, government, military, the academy, as well as worldwide. There are hundreds of thousands of cybersecurity jobs going unfilled in the US alone, and the gap will take a long time to close. Of further concern, there is anecdotal evidence that employers consider many cybersecurity graduates take too long to become effective. We need new educational models—designed specifically to develop and graduate 'breach-ready' cybersecurity professionals. One such new model is the lightweight cooperative learning model developed by CIAC at the University of Washington Bothell (Fig. 5).

Because imposing a cooperative learning structure (such as European countries have, or a few universities in the US and Canada, where a year of work interleaves a year of school) would be costly and disruptive to most academic institutions, a cybersecurity cooperative learning pilot was launched where students maintain their current academic load in the last year of their degree programs and, in addition, opt into an integrated program of professional instruction and half-time industry employment. The additional professional education includes: (1) a professional academic certificate that covers all the necessary knowledge units required to meet NSA/DHS/NIST standards and (2) a professional seminar conducted in partnership with industry to help students triage their work experience with what they've learned in the classroom. The addition of the professional seminar and certificate elements in the pilot accelerate student readiness for work when they formally graduate, based on employer and student data.

This is a public private partnership (government, industry, academia) conceived as a two-year pilot. This first year one cohort of 10 students was engaged with one employer. Students were selected based on technical foundation, interpersonal skills, team participation, and collaborative problem-solving abilities. Certificate scholarships were provided. A second year of the pilot is being conducted currently with more industry partners for the purposes of incorporating lessons learned and refining and generalizing the model for dissemination. Data collected provides insight into several questions: (1) how to scale this program, (2) how, and to what degree, this program accelerates cybersecurity job readiness, (3) what are best practices for conducting such a program.

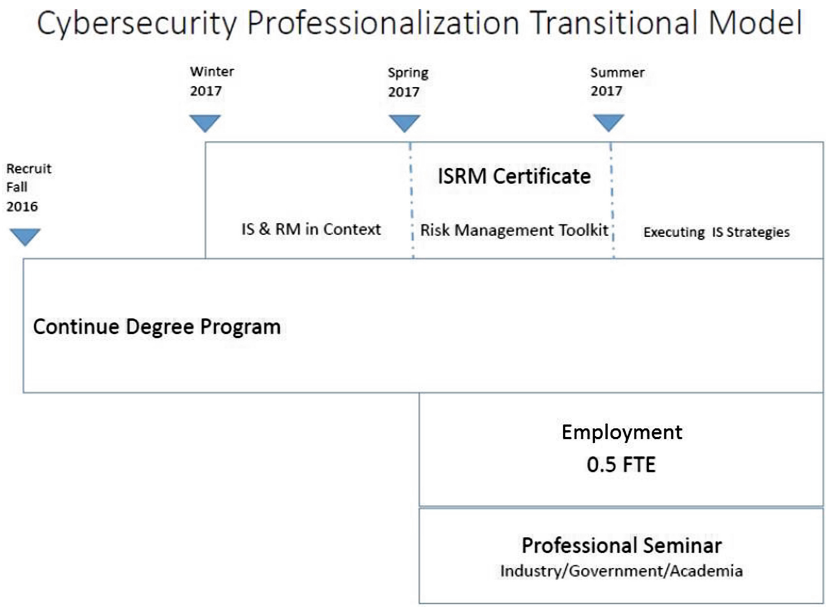


Fig. 5. Cybersecurity cooperative learning model

5 Professionalization of Cybersecurity: Standards

Complicating the issue of talent preparation, cybersecurity is professionalizing like medicine, dentistry, law, etc. Education standards are taking hold with university programs adopting curricular standards set by NIST/NSA/DHS and the emergence of ACM guidelines and ABET accreditation. The telecommunications infrastructure sector became the first to explore whether new, or additional, educational standards are necessary for cybersecurity specific to that sector through the work of the Communications Security, Reliability and Interoperability Council (CSRIC).

CSRIC reported that much of the existing work by NIST, NSA, DHS on workforce development, work roles, education standards, etc., could be leveraged by the telecommunications sector, saving time and resources and preventing balkanization of the field through separate educational standards that would isolate each sector. CSRIC also recommended a scholarship for service program for critical infrastructure given intense competition with industry that pays better for the same talent.

With commitment to truly solve the cybersecurity talent problem systemically, and provide the stable, steady funding that that would imply, it will require the kind of effort that turned the US education system around during the project to put a man on the moon that took 10 years to fix.

6 Recommendations

We've developed the technical means to protect systems, only to have those means defeated as we continually participate in an 'arms race' with online adversaries intent on their goals to defeat systems standing in the way of their objectives. The discipline of cybersecurity grew out of technical disciplines and for many years was conceived of as solvable through technical means. However, systems are composed of not only technical components, but from a systems perspective, also consist of the users, each of whom is another node in the network.

We need to do a better job of rendering the humans in the system more reliable. This is a case for developing compensating controls that will meet the security objectives of the system that remain unmet by existing tools. This includes the business and legal constraints (rules) that will contribute to de-risking systems from a cybersecurity perspective. It is the intent of CIAC to pursue research into these alternate controls, discover patterns of behavior and activity that will render the human aspects of systems more reliable and evolve standards for these practices to disseminate to others.

Acknowledgements. The author wishes to acknowledge the following organizations and individuals—representing military, industry and government, respectively—for their contributions to closing the gap in cybersecurity talent preparedness: The Washington National Guard led by Col. Gent Welsh, the Communications Security, Reliability and Interoperability Council (CSRIC) led by Bill Boni, Senior VP, T-Mobile, and the National Initiative for Education and Training Program (NIETP) at NSA led by Chief Lynne Clark.

References

1. Schroeder, S.: The Lure. Course Technology, Boston (2012)
2. Endicott-Popovsky, B., Frincke, D.: Adding the Fourth 'R': a systems approach to solving the hacker's arms race. Paper presented at Hawaii international conference on system sciences (HICSS) 39 symposium: skilled human-intelligent agent performance: measurement, application and symposium, Kauai, Hawaii, January 2006. http://www.itl.nist.gov/iaui/vvrg/hicss39/4_r_s_rev_3_HICSS_2006.doc
3. Endicott-Popovsky, B., Horowitz, D.: Unintended consequences: digital forensics literacy and the legal system. Paper presented at 65th annual scientific meeting of the American academy of forensic scientists, Washington, D.C., February 2013
4. Endicott-Popovsky, B., Endicott-Popovsky, B.: The probability of 1. J. Cyber Secur. Inf. Syst. **3**(1), 18–19 (2015)
5. Disney, W., Armstrong, S.: Fantasia [Film]. (Available from RKO Pictures 1270 Ave. of the Americas, New York, NY 10020) (1940)
6. David, S.: The Atlas of Risk Maps. CIAC, Seattle (2016)
7. Senge, P.: The Fifth Discipline. Doubleday, New York (2006)
8. Rand Corporation: Cyber Power Potential of the Army's Reserve Component (2017). https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1490/RAND_RR1490.pdf
9. Schmitt, M. (ed.): The Tallinn Manual on the International Law Applicable to Cyberwarfarre. Cambridge University Press, New York (2006)