CYBERSECURITY WHITEPAPER:
A CALL TO ACTION at PSU to HELP OREGON and USA

PREPARED BY

Dr. Birol Yeşilada, Director NCAE-C

Dr. Barbara Endicott-Popovsky

Dr. Tuğrul Daim

Susan Tardif, Senior Executive Assistant

Mark O. Hatfield School of Government

(January 2022)

"Unless we have well-educated people, we're vulnerable on our national security."
Senator Mark O. Hatfield

EXECUTIVE SUMMARY

The purpose of this White Paper is to provide a brief overview of PSU's cybersecurity vision, initiatives, and Call to Action for Portland State University (PSU) and The State of Oregon. In June 2020, PSU became a National Center of Academic Excellence in Cybersecurity (NCAE-R) designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS). In August 2021, our center received a $3 million multi-year grant from the NSA to evaluate cybersecurity energy-critical structure and workforce shortcomings in the Pacific Northwest and help formulate intra- and inter-state cybercommunity community consortium of academia-government/public-industry/private partnership to find solutions to these challenges. The Hatfield School leads the coordination of cybersecurity initiatives of PSU, and I serve as the Director and person of contact for NSA and DHS.

The information age has brought unprecedented advances to societies as well as challenges. Increasingly, Cybersecurity and Cyber Defense have become daily challenges for governments, industries, organizations, and individuals, among others. Advances in information technologies (ITT) have been a blessing and a liability. Today, ITT technologies enable humanity to be more productive, connected, and informed. At the same time, state and non-state actors use advanced technologies to launch attacks against military, governmental, and civilian targets with an ever-increasing cost. Cyber-attacks can take physical and nonphysical forms. Our foreign adversaries and, to some extent, domestic groups increasingly employ *social engineering* to manage social change and regulate society's future growth and behavior. Western democracies' unique blend of open economies and political systems enable these enemies of democratic countries to penetrate and destabilize them.

Meeting these challenges requires a bold new approach to educating our students and training the workforce in Cybersecurity. This is because no single academic discipline or program can address all angles of the complex cyber world. In other words, as long as academic units remain in silos, we will not be able to attain a systems view, a holistic approach, to cyber studies and Cybersecurity. While the technical aspects of cybersecurity research and development (R&D) became a priority, this resulted in an overemphasis on cyberstudies' technical sciences and engineering side. At the same time, the human factor remained focused on technological and software engineering capabilities. The result is a widening gap between technology-related fields and "soft" sciences.

In this White Paper, we outline the nature of our nation's threats, shortcomings in addressing these challenges and propose the blueprint for a new vision for a cooperative partnership between academia, government, and industry for education and workforce training in Cybersecurity cyber defense.

CONTENTS:

BRIEF

Portland State University (PSU) has been designated as a **National Center of Academic Excellence in Cyber Research** (CAE-R) by the National Security Agency (NSA) and the Department of Homeland Security (DHS). PSU's excellence in Public Affairs education, workforce training, and community engagement in solving policy challenges, Computer Sciences and Engineering, and Business Administration presents a unique opportunity to build cross-disciplinary collaboration among faculty and students in the Cybersecurity and cyber defense fields. In 2021, we also applied for the Center in Cyber Defense Education (CAE-CD) designation by NSA and DHS. Professor Birol Yeşilada, Director of the Mark O. Hatfield School of Government, is the contact for CAE-R for NSA and is appointed by Provost Jeffords as Director of PSU's Cybersecurity Coordinating Taskforce.

President Steve Percy and Provost Susan Jeffords charged the Cybersecurity Taskforce to develop university-wide comprehensive and diverse Cybersecurity and cyber defense programs for education and workforce training. This is not considered a substitute for our existing programs in individual Colleges and Departments. Instead, we will design interdisciplinary degree programs and certificates to complement existing programs through synergies of collaboration across PSU's departments.

At the Mark O. Hatfield School of Government, we created **The Mark O. Hatfield Center for Cybersecurity** as a collaborative partnership of PSU Colleges and Schools dedicated to bringing together scholars, industry partners, and policymakers to train students and translate research findings into effective policy for Cybersecurity and cyber defense. This is a requirement for the CAE-R designation by the NSA for coordination/information clearinghouse purposes. Information from NSA/DHS/NSF, such as educational and research grant opportunities, invitations for collaborations with other institutions around the country, and conferences, come to this contact center and are shared with the participating units and faculty across PSU.

Housed within PSU's Center for Public Service (CPS), the Mark O. Hatfield Center for Cybersecurity strives to contribute to regional and national efforts to further cybersecurity expertise and education in ways that complement and enhance national goals and investments. It is in the interest of our national security that local governments be prepared to defend themselves from cyber-attack. PSU's Mark O. Hatfield Center for Cybersecurity distinguishes itself from other CAE-R centers by shifting the focus from the federal level to prioritizing America's small and regional governments' cyber defense and emphasizes the need **to build a bridge between technology (computer sciences and engineering), collaborative governance, public policy, and public awareness.** We can better achieve these goals in ***partnership with*** our

partner higher education institutions, Oregon State University, University of Oregon, and CAE designated Community Colleges (Chemeketa CC, Mt. Hood CC, and PCC).

PSU faculty follow the university's motto, **"Let Knowledge Serve the City,"** to pursue scholarship in an applied setting. This promotes an interdisciplinary approach to research and a particular commitment to community engagement. Our partners include government institutions, high-tech companies, and other higher education institutions.

This is important for PSU's leadership team and Oregon's elected officials and industry leaders to emphasize. Cybersecurity and cyber defense studies are growth areas for Oregon and the Pacific Northwest. Whereas the Mid-Atlantic and East Coast are very dense with cybersecurity offerings, the Northwest is a greenfield and wide-open for innovative ideas.

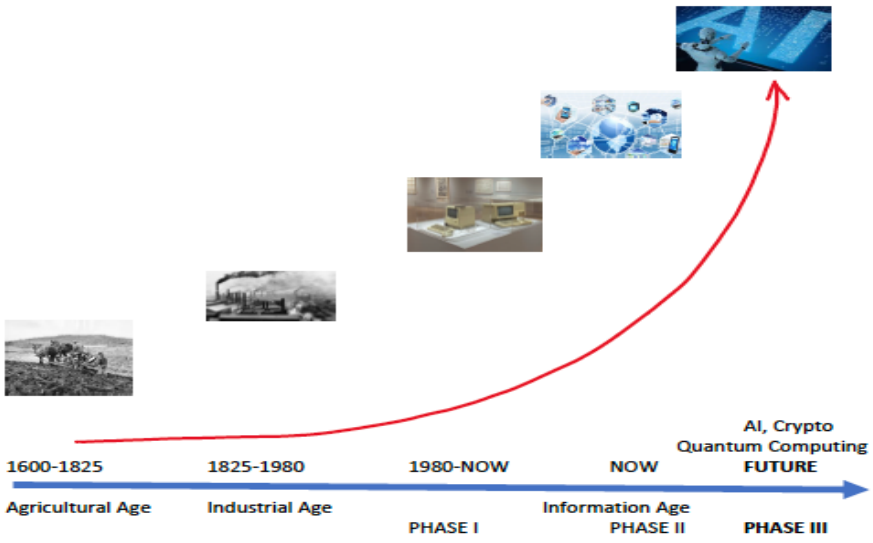
PSU's unique collaborative and interdisciplinary approach to cyber defense and Cybersecurity breaks down the traditional communication barriers between technology and public affairs experts and serves the purpose of supporting state and local governments, private companies, and federal institutions. Our research in applied context provides expertise to K-12 educators to get students interested in topics relevant to Cybersecurity, the training of future researchers and practitioners in the private and public sectors, providing policy advice to public officials, and technical expertise to defend better our industries and the public sphere (including elections) against cyberattacks.

THE NATURE OF THE PROBLEM

According to the Association for Computing Machinery, Cybersecurity (CSS) includes managing risks related to the use, processing, storage, and transmission of information and the systems and processes used for those purposes, including analog and physical form. CSS includes information availability, identification, and authentication, confidentiality, integrity, and non-repudiation, as well as the economic considerations concerning the selection of CSS techniques, CSS processes, and industry trends. Cybersecurity Education typically considers Cybersecurity as a computer-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries (individuals and states). While the technical aspects of cybersecurity research and development (R&D) became a priority, this resulted in overemphasis on cyberstudies' technical sciences and engineering side. At the same time, the human factor remained focused on technological and software engineering capabilities. The result is categorized silos and a widening gap between technology-related fields and "soft" sciences. Threats in the cyber world typically involve ransom attacks, malware, and phishing. However, recent developments also show that our foreign adversaries and, to some extent,

domestic groups increasingly employ *social engineering* to manage social change and regulate society's future growth and behavior. Western democracies' unique blend of open economies and political systems enable these enemies of democratic countries to penetrate and destabilize them. **The grave threat we face as a nation requires a holistic or systems approach to cybersecurity education**. Figure 1 provides the progression of industrial and technological advancement that brought us to the information age and its challenges.

Figure 1: Where We've Been and Where We're Going



This progress also resulted in dramatic shifts in criminal elements and enemies' abilities to target individuals, industries, and governments for gains and, in return, adjustments in defense mechanisms (as shown in Table 1). In no uncertain terms, these developments constitute severe challenges for all concerned, whether individuals, institutions, private companies, large corporations, NGOs, or governments (local to national).

Table 1: The History of Cyberconflict

Stages	Realization	Takeoff	Militarization
Timeframe	1980	1998–2003	2003–present
Dynamics	Attackers have advantage over defenders	Attackers have advantage over defenders	Attackers have advantage over defenders
Who Has Capabilities?	United States and few other superpowers	United States and Russia with many small actors	United States, Russia, China, and many more actors with substantial capabilities
Adversaries	Hackers	Hacktivists, patriot hackers, viruses, and worms	Neo-Hacktivists, espionage agents, malware, national militaries, spies, and their proxies, hacktivists
Major Incidents	Cuckoos Egg (1986), Morris Worm (1988), Dutch Hackers (1991), Rome Labs (1994), Citibank (1994)	Eligible Receiver, Solar Sunrise, Moonlight Maze, Allied Force, Chinese Patriot Hackers	Titan Rain, Estonia, Georgia, Buckshot Yankee Stuxnet
US Doctrine	Information warfare	Information operations	Cyber warfare

Jason Healey, ed. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna, VA: Cyber Conflict Studies Association, 2013).

There is no denying that daily constraints such as budgetary limitations and personnel shortages are compounded by shifting legislative priorities and the onslaught of cyberattacks at every government level. Local governments and private end-users of cyber-vulnerable industries connected to critical infrastructures represent soft targets for our adversaries to attack and disable America's complex sectors through our soft underbelly. Our proposed scheme addresses these challenges. We should anticipate capitalizing on the current interest that regional, state, local officials, industry, and academia have for Cybersecurity to support participation in risk assessment for critical infrastructure design and plan alternative solutions, and carry out training and preparedness activities for participants from consortium partners.

With social engineering as a compounding factor, adversaries can take advantage of local access points to sensitive data and information networks for more targeted attacks. After a recent breach at Oregon's Department of Human Services, Gary Johnson, Oregon's Chief Information Security Officer, has worked across state agencies to raise awareness and formalize

protocols to avert future attacks. "People will still be the most vulnerable risk to any organization and will be for the foreseeable future, but with the right kind of education and training, they can also serve as the first line of defense."[1]. Although policymakers at the national level have tracked advancements in Cybersecurity and cyber defense, localized policy prescriptions and technical solutions have not progressed at the same rate. NCAE's university consortium uniquely addresses these growing threats and gaps to raise awareness and leverage resources across multi-sector actors. Without collaboration, technology often outpaces its regulatory environment, resulting in unforeseen complications. We can identify several problems in our current approach to Cybersecurity and cyber defense, which serve as drivers to our proposals in this White Paper.

PROBLEM 1: A Severe Shortage of Cybersecurity Professionals

- The cybercrime epidemic has escalated rapidly in recent years, while companies and governments have struggled to hire enough qualified professionals to safeguard against the growing threat.
- This trend is expected to continue into 2020 and beyond, with some estimates indicating some 1 million unfilled positions worldwide (potentially rising to 3.5 million by 2021).
- The gap between *TECHNOLOGY and HUMAN CAPITAL.*

The cybercrime epidemic has escalated rapidly in recent years, while companies and governments have struggled to hire enough qualified professionals from diverse backgrounds to safeguard against the growing threat. This trend is expected to continue into 2021 and beyond, with some estimates indicating shortages of up to 1 million unfilled positions worldwide since 2014, quickly rising to an estimated 3.5 million[2] today. Studies show that organizations with racially and ethnically diverse leadership teams benefit both company culture and bottom-line revenues while also increasing overall confidence in an organization's security posture[3].

Our proposal is designed for optimizing experiential learning and fellowships to accelerate and diversify the opportunity for up-and-coming cybersecurity professionals. Bridging opportunities to Science, Technology, Engineering, Arts, and Mathematics (STEAM) fields of study and career paths for women and people of color has been a critical movement in the PNW Region over the last fifty years. In Cybersecurity, the lack of cultural representation creates national security risks - limited perspectives more quickly devolve into groupthink. There is an urgent need to build the

[1] https://www.govtech.com/security/Oregon-Sharpens-Cyberdefenses-in-the-Month-After-DHS-Breach.html
[2] https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html
[3] https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx

pipeline from K-12 to employment through engaging hands-on experience, education, and training. Racial and ethnic diversity in the intelligence community enhances U.S. national security. Security and equity are paramount in addressing the complexity of soft and hard sciences needed to identify and decode cybercriminals' evolving agendas. By attracting women and people of color to Cybersecurity, our proposal creates a more secure network and the necessary tactical and operational workforce to defend our shared assets.

PROBLEM 2: A Severe Vulnerability of Local and County Governments and FEMA, DHS, CISA Regions - America's Soft-Underbelly

- There are over 89,000 local governments in the U.S. Furthermore, they are within the Cybersecurity and Infrastructure Security Agency (CISA) regions. **CISA** is a standalone United States federal agency, an operational component under Department of **Homeland Security** (**DHS**) oversight. CISA delivers services to support the security and resilience of critical infrastructure owners and operators and state, local, tribal, and territorial partners through 10 regions, inclusive of all states and territories. Regional personnel works with critical infrastructure partners and communities at the regional, state, county, tribal, and local levels to:
    - Support preparation, response, and recovery efforts for hazards that impact critical infrastructure.
    - Safeguard soft targets and crowded places.
    - Conduct and integrate infrastructure assessments and analysis, including dependencies and cascading effects, on critical infrastructure to influence decision-making at all phases of emergency management.
    - Facilitate information sharing between public and private sector critical infrastructure partners.
    - Enhance election infrastructure security and other critical infrastructure cyber systems.
    - Improve situational awareness of cybersecurity risks and incidents.
- The table below provides an overview of local and regional entities vulnerable to cybersecurity threats in Oregon, Washington, and Idaho, which require more attention and intentionality to align with federal resources through the NCAE-C NW Region.

Table 2. OR, WA and ID Local and Regional Entities

Oregon	Washington	Idaho
240 municipalities	281 municipalities	200 municipalities
36 County governments	39 County governments	44 County governments
230 School Districts	295 School Districts	115 School Districts
1,004 Special Districts	1,700 Special Districts	1,556 Special Districts

PROBLEM 3: Education Gap

- **Develop Evidence-Based Policy Recommendations and a Technology Roadmap (TRM) to Improve Cybersecurity Whole of State System Strategy**

Cybersecurity Education typically considers computer-based disciplines involving technology, information, and processes to enable assured operations in the context of adversaries (individuals and states). The result is categorized silos and a widening gap between technology-related fields and "soft" sciences. Cybersecurity threats must be managed with more agility and sensitivity to the ideological, cultural, and societal risks that drive new risk factors to move towards more collaborative governance and shared responsibility across society. Recent cyberattacks show that our foreign adversaries and, to some extent, domestic groups increasingly employ ***social engineering*** to manage social controls, change, and regulation of individual and societal behaviors. To move towards a whole state cybersecurity approach, we'll expand efforts for a multidisciplinary response to combat threats arising from social engineering from domestic and foreign adversaries.

Analysts in front of a computer terminal or listening to voice recordings need to distinguish between genuine and phony adversaries (including one adversary pretending to be another), understand hidden meanings behind allegory and symbolism, and differentiate between cultural signals such as accents and speech patterns. The grave threat we face as a nation requires a

holistic or systems approach to cybersecurity policy and education. We build a bridge between technology and "soft" sciences to address the human capital and capacity gap.

When addressing the challenges of Cybersecurity, cyber defense, education, and workforce training, it is crucial to stress the core values and guiding principles of NCAE-C.

- **The Ethical Behavior Core Value:** The academic institution must encourage and support ethical behavior by students, faculty, administrators, and professional staff.
- **The Shared Core Value:** The institution enables an environment in which students, faculty, administrators, and professional staff, and practitioners can share, interact, and collaborate with others in the cybersecurity field.
- **The Lead by Example Core Value:** The institution demonstrates a commitment to address, engage, and respond to current and emerging cybersecurity issues in the classroom, the institution itself, and outside the institution.

PROBLEM 4: Russia, China, Iran, North Korea, and other foreign adversaries of the USA

Adversaries of the U.S. and Western Allies increasingly resort to cyberwarfare in their attempt to undermine American democracy and national security. Western democracies depend on multilateral networks built on open economic and political systems, turning into a target-rich environment for counter forces to penetrate and destabilize. Russia, China, Iran, North Korea, and other foreign adversaries to the U.S. and Western Allies increasingly resort to cyberwarfare in their attempt to undermine American democracy and national security. The Belfer Center of Harvard Kennedy School's National Cyber Power Index identifies China and Russia explicitly within the top ten global powers with comprehensive cyber capabilities. Their efforts undermine physical infrastructures, democratic processes and drive a wedge between citizens through social media networks[4]. About cyber warfare capabilities, the U.S. Department of Defense Science Board's report *Resilient Military Systems* classifies it in these six tiers (TABLE 3):

[4] House Hearing, 113 Congress, http://www.gpo.gov/fdsys/ and Q.E. Hodgson, L. Ma, K. Marcinek, and K. Schwindt, *Fighting Shadows in the Dark,* RAND 2019

TABLE 3: Six Tiers of Cyberwarfare

TIER 1	The cyber actor(s) possess extremely limited technical capabilities and largely makes use of publicly available attack tools and malware. Sensitive data supposedly leaked by the attackers are often linked back to previous breaches and publicly available data.
TIER 2	Attackers can develop rudimentary tools and scripts to achieve desired ends in combination with the use of publicly available resources. They may make use of known vulnerabilities and exploits.
TIER 3	Actors maintain a moderate degree of technical sophistication and can carry out moderately damaging attacks on target systems using a combination of custom and publicly available resources. They may be capable of authoring rudimentary custom malware.
TIER 4	Attackers are part of a larger and well-resourced syndicate with a moderate-to-high level of technical sophistication. The actors are capable of writing custom tools and malware and can conduct targeted reconnaissance and staging prior to conducting attack campaigns. Tier 4 attackers and above will attempt to make use of publicly available tools prior to deploying more sophisticated and valuable toolkits.
TIER 5	Actors are part of a larger and well-resourced organization with high levels of technical capabilities such as those exhibited by Tier 4 actor sets. In addition, Tier 5 actors have the capability of introducing vulnerabilities in target products and systems, or the supply chain, to facilitate subsequent exploitation.
TIER 6	Nation-state supported actors possessing the highest levels of technical sophistication reserved for only a select set of countries. The actors can engage in full-spectrum operations, utilizing the breadth of capabilities available in cyber operations in concert with other elements of state power, including conventional military force and foreign intelligence services with global reach.

The impact of cyber-attacks include:

NEGLIGIBLE	Damage from these attacks is highly unlikely or is unable to adversely affect the targeted systems and infrastructure. Such incidents may result in minor reputational damage. Sensitive systems and data remain intact, confidential, and available.
LOW	Attacks have the capacity to disrupt some non-critical business functions, and the impact is likely intermittent and non-uniform across the user base. User data and sensitive information remain protected.
MODERATE	Attacks have the potential to disrupt some core business functions, although the impact may be intermittent and non-uniform across the user base. Critical assets and infrastructure remain functional, even if they suffer from moderate disruption. Some non-sensitive data may be exposed. Actors at this level might also expose sensitive data.
SEVERE	Cyber attacks at this level have the capacity to disrupt regular business operations and governmental functions severely. Such incidents may result in the temporary outage of critical services and the compromise of sensitive data.
CATASTROPHIC	Kinetic and cyber attacks conducted by the threat actor(s) have the potential to cause complete paralysis and/or destruction of critical systems and infrastructure. Such attacks have the capacity to result in significant destruction of property and/or loss of life. Under such circumstances, regular business operations and/or government functions cease and data confidentiality, integrity, and availability are completely compromised for extended periods.

http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

The Belfer Center of Harvard Kennedy School's National Cyber Power Index also identifies China and Russia within the top ten global powers with comprehensive e cyber capabilities (https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf).

Russia

Russia, under Putin, has been engaged in a multi-pronged war with the West since the late 1990s. On the one hand, the Russian military and its proxies destabilized and occupied parts of former Soviet republics (i.e., Georgia and Ukraine) and engaged in direct military operations in Russia's periphery (like Syria). At the same time, Vladimir Putin employed information warfare to undermine Western democracies. This is a complex military doctrine that western democracies did not recognize until Russian cyber armies successfully interfered in democratic elections.

Using the term "information warfare" in American public discourse to describe Russia's interference in other countries' internal political affairs is problematic. This is partly due to the operationalization of information warfare in the United States, bound by the confines of legal and cultural barriers. Russia not only faces fewer legal and cultural obstacles to influence at the operational and strategic level during both war and peace, but it also has philosophically different approaches and goals while operating in the information environment. Aleksander Dvornikov, commander of Russia's Southern Military District, points out:

> "Now, states achieve their geopolitical goals by applying complex non-military measures, which often are more effective than the military ones. The main goal of these measures is not the physical destruction of the enemy but the complete submission of his will."
> (Aleksandr Dvornikov, "Штабы для новых войн," Военно-промышленный курьер, 23 July 2018. Russian publication *Military-Industrial Courier*).

He argues that Russia would not have succeeded in many operations in Syria and elsewhere without information operations. To summarize the Russian threat:

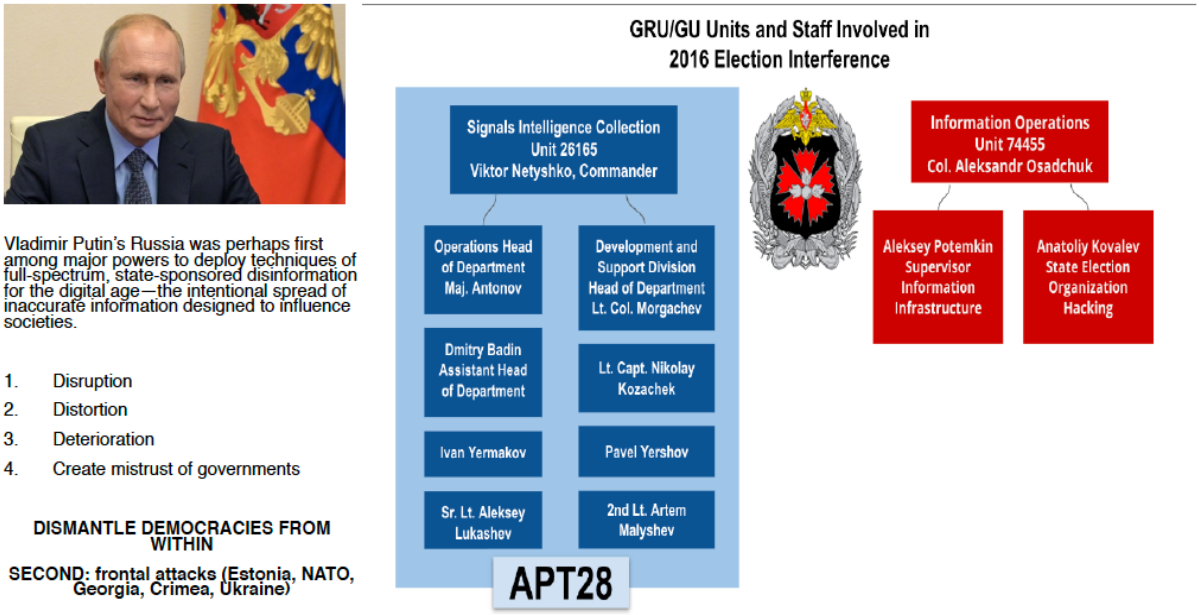
- The Russian approach is holistic. It aims to affect the target state and its armed forces and achieve desired effects in the mind of target populations' perceptions and decision-making processes that favor Russia's interests and goals. For the Russians, *END JUSTIFIES THE MEANS.* They will use any method to achieve their goals (social media, hacking, etc.).

- This two-pronged approach seeks to affect both the physical and cognitive dimensions of the information environment.

- At the physical level, what the Russians call the digital-technological level, they seek to disrupt and compromise the physical dimension of the information environment by penetrating, manipulating, and destroying information networks and command and control systems.

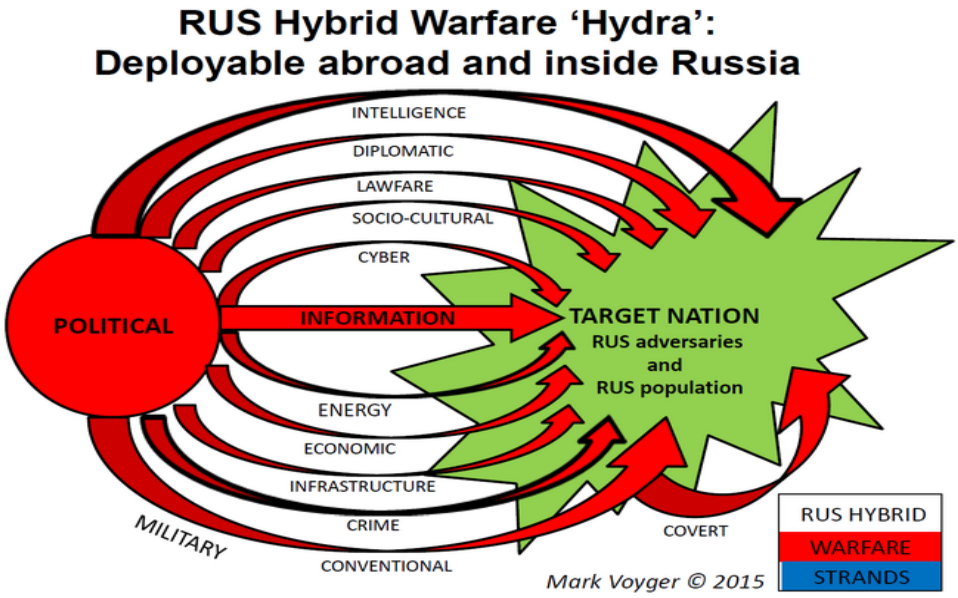
- At the cognitive level, the Russians have already demonstrated the ability to integrate actions in the physical dimension of operations in the information environment with activities intended to affect perceptions and decision-making processes; in other words, they are achieving effects on the cognitive side. Figure 2 provides this complex network of Russian information warfare doctrine against democracies.

Figure 2: Russian Information Warfare Framework



A more detailed description of the Russian cyber-attacks is provided by Mark Voyger, former special advisor to retired Lieutenant-General Ben Hodges, former Commanding General of U.S Army Europe, in Figure 3. Recently, the U.S. government accused Russia in January of hacking nine government agencies via SolarWinds, a Texas software company widely used by American businesses and government agencies.

Figure 3: Russian Cyber
(https://news.postimees.ee/4505726/mark-voyger-russian-hybrid-warfare-can-still-bring-surprises-in-the-future)



China, North Korea, and Iran

China has directly utilized its information via cyber espionage to improve its military capabilities. It has also used ill-gotten trade secrets to help its commercial companies compete globally. Chinese corporations have successfully generated business in the developing world, building partnerships and promoting Chinese brands throughout Africa and the Middle East. For example, telecommunications giants Huawei and ZTE have already gained significant market share in Africa, partially due to multi-faceted support from the Chinese government. However, the prospect of having Chinese hardware built into telecommunications systems, particularly the emerging 5G cellular networks, has raised significant concerns over potential cyber espionage within the U.S. government. These concerns prompted the United States to ban 5G technology from Chinese manufacturers within its borders. They have encouraged allies to do the same (for more information, see https://securityboulevard.com/2020/12/china-cyber-attacks-the-current-threat-landscape). China is no longer a second-tier cyber threat to Western democracies. It now has one of the world's most preeminent cyber armies and quickly taking over Russia as our primary adversary.

According to Kevin Collier, "China is behind a newly discovered series of hacks against key targets in the U.S. government, private companies, and the country's critical infrastructure, cybersecurity firm Mandiant said Wednesday. The hack works by breaking into Pulse Secure, which businesses often use to let workers remotely connect to their offices. The campaign is the third distinct, severe cyberespionage operation against the U.S. made public in recent months, stressing an already strained cybersecurity workforce. (https://www.nbcnews.com/tech/security/china-another-hack-us-cybersecurity-issues-mount-rcna744). In March, Microsoft blamed China for starting a free-for-all where scores of different hackers broke into organizations around the world through the Microsoft Exchange email program."

North Korean hackers have also become a significant threat in the cyberworld. They've stolen billions of dollars. They paralyzed the United Kingdom's National Health Service and hacked India's newest nuclear power plant to steal its designs. The United States Department of Justice has charged three North Korean computer programmers with various cyber-attacks that made headlines worldwide.
The men – 31-year-old Jon Chang Hyok, Kim Il, 27, and 36-year-old Park Jin Hyok – are alleged to have been part of North Korea's Reconnaissance General Bureau (RGB), known commonly as the "Lazarus Group" or "APT38", tasked with criminal hacking operations. (https://www.tripwire.com/state-of-security/featured/us-charges-north-korean-hackers-wannacry-sony-pictures-attack/).

The Cybersecurity and Infrastructure Security Agency (CISA) issued a warning to be vigilant for Iranian hackers' activity. The notification stated that "Iranian cyber threat actors have been continuously improving their offensive cyber capabilities, … They continue to engage in more conventional offensive cyber activities ranging from website defacement, distributed denial of service attacks, and theft of personally identifiable information, to more advanced activities—including social media-driven influence operations, destructive malware, and, potentially, cyber-enabled kinetic attacks." (https://www.nextgov.com/cybersecurity/2020/12/cisa-warns-irans-offensive-cyber-capabilities/170505/)

In addition to foreign governments, terrorists and extremist groups today use the power of the Internet, especially social media, to spread their messages of hate and intolerance, and to recruit new members, often targeting vulnerable young people. The global reach of cyberspace and its complexity provide bad actors ample places to hide, safe from the reach of international law.

ACTION ITEMS: How Should We Respond to Cybersecurity and Cyber Defense Needs at PSU?

A BOLD INITIATIVE TO MEET THE CHALLENGES: INTERDISCIPLINARY AND COLLABORATIVE APPROACH TO CYBERSECURITY

WHY?

Serious shortcomings make it imperative for Oregon to create a collaborative educational and workforce training environment that brings together government, higher education, and industry to defend Oregonians and the nation against cyberattacks. No single institution of higher education has sufficient resources to address these problems on its own. A ***collaborative strategy*** *is necessary: a partnership between academia, government, and industry. The National Initiative for Cybersecurity Education (NICE) identifies competency, skills, diversity, task orientation, and sustainability as critical educational and workforce training priorities. This can only be achieved through a true partnership of academia, government, and industry.*

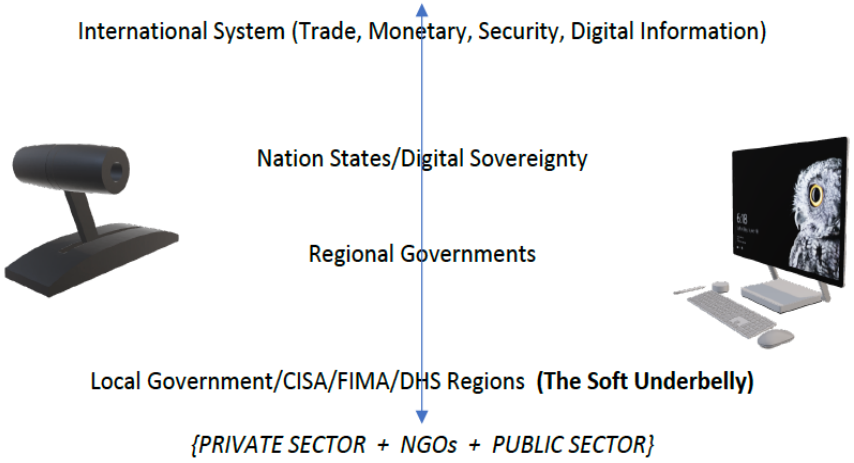
Next Frontier for Closing the Cybersecurity Skills Gap: A Case for a New Approach

Build a bridge between High-Tech and Public Policy & Analysts to close the gap between engineering/computer sciences and the soft sciences (cognitive, humanities, public policy).

- Horizontal and Vertical integration of analysis (local to global AND public-private)
    - Local to Global levels of analysis of threats (integrated approach)
    - A public-private partnership of key stakeholders (K-12, academia, government, and industry)
    - Interdisciplinary and multi-tools training of students.
    - Emphasis on competency measures, skill development, diversity, and learning application.

National Cybersecurity involves a systemic understanding of how each component interacts with the others. In other words, the local level of security is not an isolated matter because, in the cyber world, all levels of analysis become connected through data networks – local through international. Moreover, information technologies education and technical approach to Cybersecurity can only be as good as human information embedded in its system. In other words, Cybersecurity without humans is a limited asset. This approach, see Figure 4, requires integrating the analysis levels (vertical integration from local to the international system) and horizontal integration of all stakeholders (individuals, government, and industry).

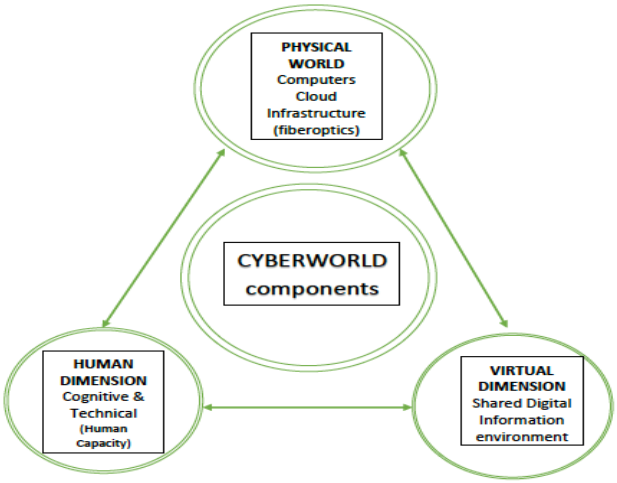
Figure 4: Horizontal and Vertical Integrative Education, Research, and Workforce Training



We also need to form bridges across traditional disciplines in terms of educational expertise for workforce training. If Computer Sciences and Engineering is one side of the coin, humanities and social sciences make up the other. That is what holistic approach cybersecurity and cyber

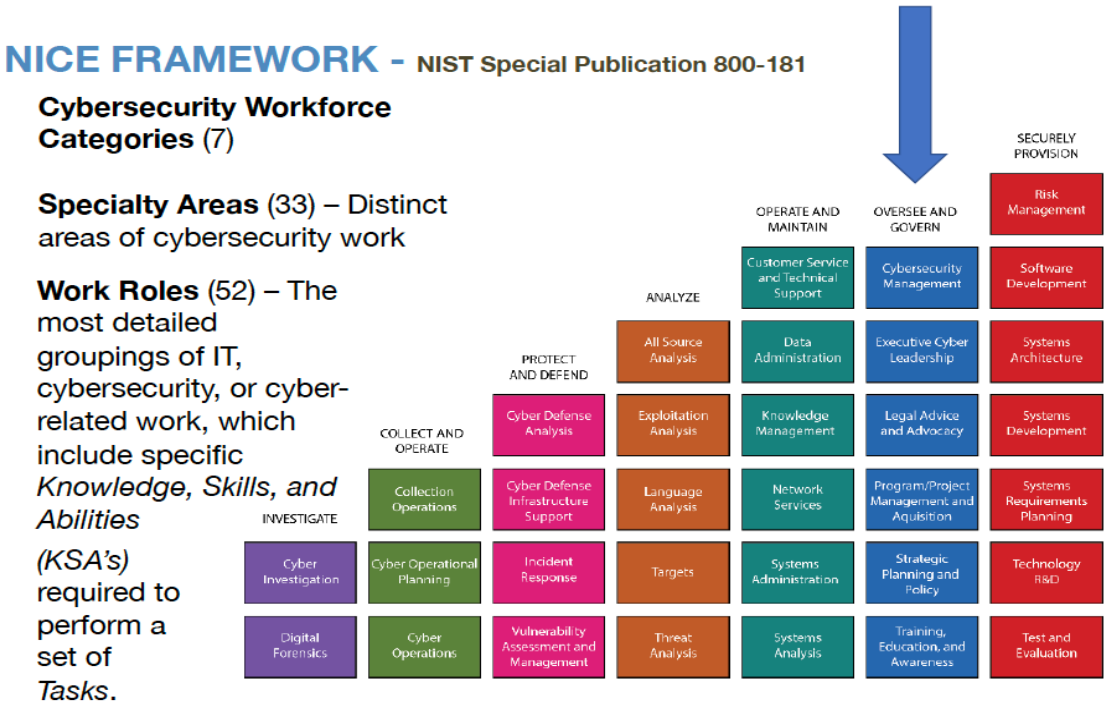
defense require. A bridge between technology and other disciplines is necessary as the cyber world becomes more complex (see Figure 5). This need has been identified as a priority in the National Initiative for Cybersecurity Education (NICE).

Figure 5: An Interdisciplinary Framework



NICE Framework for cybersecurity education expanded to include several areas of expertise, as shown in Table 4.

Table 4: The Nice Framework



And Categories' Description

Categories	Descriptions
Securely Provision S.P.P)	**Conceptualizes, designs, and builds secure information technology I.T.T) systems, responsible for aspects of systems and/or networks development.**
Operate and Maintain O.M.M)	**Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology I.T.T) system performance and security.**
Oversee and Govern O.V.V)	**Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.**
Protect and Defend P.R.R)	**Identifies, analyzes, and mitigates threats to internal information technology I.T.T) systems and/or networks.**

Analyze (AN)	**Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.**
Collect and Operate C.O.O)	**Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.**
Investigate (IN)	**Investigates cybersecurity events or crimes related to information technology I.T.T) systems, networks, and digital evidence.**

The section on Oversee and Govern includes many underemphasized areas in cybersecurity education as shown in Table 5.

Table 5: Oversee and Govern (6 Specialty Areas and 14 Work Roles)

Category	Specialty Area	Work Role
Oversee and Govern	Legal Advice and Advocacy	Cyber Legal Advisor
		Privacy Officer/Compliance Manager
	Training, Education, and Awareness	Cyber Instructional Curriculum Developer
		Cyber Instructor
	Cybersecurity Management	Information Systems Security Manager
		Communication Security Manager
	Strategic Planning and Policy	Cyber Workforce Developer and Manager
		Cyber Policy and Strategy Planner
	Executive Cyber Leadership	Executive Cyber Leadership
	Program/Project Management and Acquisition	Program Manager
		IT Project Manager
		Product Support Manager
		IT Investment/Portfolio Manager
		IT Program Auditor

Our proposed emphasis on an interdisciplinary educational framework meets current and future requirements in Cybersecurity:

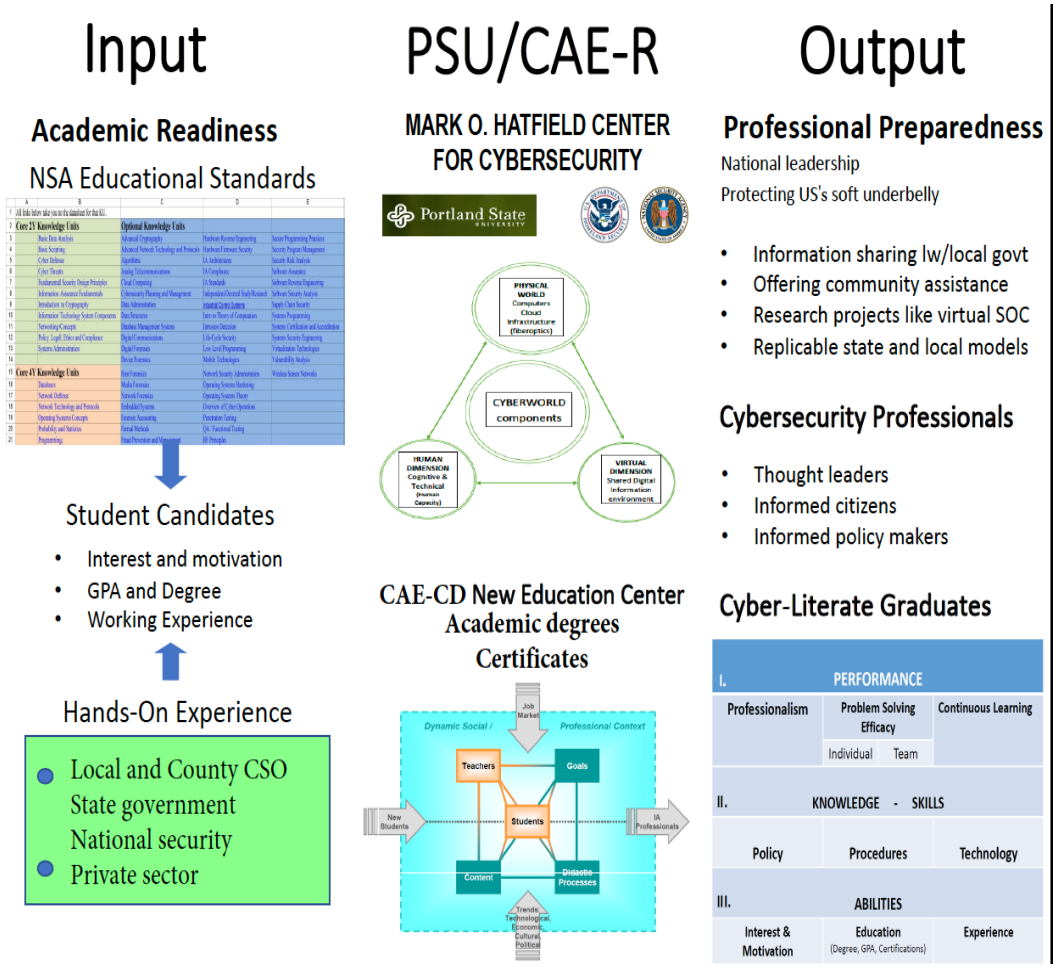
- Follow the Academic Readiness criteria of NICE to meet national standards outlined by the National Centers of Academic Excellence in Cybersecurity. Emphasis is placed on competency, knowledge, skills, and task management:
    - **Goal 1:** Establish a sustainable, diverse pipeline of students for education and workforce training through a partnership of academia, government, and industry.
    - **Goal 2:** Quality, collaboration, and innovation; Conduct competitions for community development and student competency development.
    - **Goal 3:** Partnership with industry to support apprenticeships and cooperative education.
    - **Goal 4:** Establish a sustainable pipeline of students K12 through universities and create a collaborative network of institutions across Oregon.
    - **Goal 5:** Utilize NSA's Federal Virtual Training Environment (FedVTE) for self-paced learning.

In preparing for Holistic Cyberwarfare, we recognize the following:

- Our local governments are at the most significant risk of cyber-attacks - the soft underbelly of the USA.
- Most federal legacy systems need modernization.
- Russia conceptualizes cyber operations within the broader Framework of information warfare.
    - Russia's two-pronged approach seeks to affect both the physical and the cognitive dimensions of the information environment.
- There must be workforce training above and beyond ITT, Engineering, and Computer Science.
- Identified Vulnerabilities:
    - Networks Poor physical security, management, port security, Firewall, anomaly detection.
    - Configuration Poor account management, passwords, patch management, ineffective detection programs
    - Platforms lack of system update, insecure applications, untested third-party applications, patch management
    - Public Policy (Domestic and National Security) Inexperience personnel, inadequate security awareness, insufficient training for social engineering recognition, physical security, weak access control, outdated policies

Figure 5 outlines this integrated and interdisciplinary model.

Figure 5. A Comprehensive Model for Integrated and Interdisciplinary Approach to Cybersecurity Education



Our foreign adversaries and cybercriminals learn to use an insidious method in cognitive psychology by playing to our biases. Cognitive biases are often a result of your brain's attempt to simplify information processing through our belief system and cybernetic networks. They can determine a person's perceptions and misperceptions of information. A person influenced by various biases and presented with a particular framing of an issue can easily accept distorted thinking like belief in conspiracy theories. Different fringe groups, political activists, foreign adversaries, and mainstream political parties have employed such framing tools to shape the hearts and minds of the general public through social media and other information mechanisms. Research suggests that cognitive training that includes linguistics and cognitive neuroscience can help minimize biases in decision-making. Neuroscience impacts every side of

the digital environment, i.e., Artificial Intelligence, and scientists have recognized in recent times that neuroscience without a cognitive brain is only part of the larger picture. Furthermore, the relationship between computing and cognition emerged as early as the 1950s during the behavioral revolution in social sciences. Today, one can find the need for cognitive science in every aspect of Cybersecurity. For example, see an influential article by Anne-Laure Sellier, Irene Scopelliti, and Carey Morewedge, "Debiasing training improves decision making in the field," *Psychol Sci*. 2019;30(9):1371-1379 and Amos Tversky and Daniel Kahneman. "Judgment under Uncertainty: Heuristics and Biases." Science (September 1974) 185:1124-31.

The ability to educate and train students to tackle such complex challenges requires blending relevant disciples. As Robert Axelrod of the University of Michigan outlines, we can see how these all affect decision-making in the context of issue framing (from PS 793 Syllabus):

> Political science (campaign politics and foreign policy decision making),
> Cognitive psychology (e.g., sensemaking, attribution, and inference),
> Social psychology (e.g., cognitive consistency and social influence),
> Anthropology (e.g., shared culture and ethnocentrism),
> Economics (e.g., the "hidden hand" frame),
> Business (especially advertising),
> Sociology (e.g., social mobilization), and
> Artificial Intelligence (case-based reasoning).

Combined, these knowledge bases would enable us to build bridges between technical and "soft" sciences fields. This is desperately needed in the current environment.

The building blocks for a capable and ready Cybersecurity Workforce that captures K12-university education is a priority for NSA/DHS/NSF for funding opportunities. As an NCAE institution, PSU is uniquely positioned to play a leadership role in the region to advance its educational mission.

In its entirety, this approach moves beyond academic education. It combines ***task, knowledge, and skills (TKS)*** as the competency requirements for sustainable workforce education and training to meet growing demands in the job market. Figure 7 outlines the essential steps for defining competency outlined by NICE and Competency-Based Education Network.

Figure 6: Competency Defined

Source: Charla Long, Executive Director, Competency-Based Education Network, NICE Symposium, December 16, 2020.

This model meets priority areas of education and research support of NSA's NCAEs.

- Healthcare
- Modular Approach to CLOUD Security
- Encrypted Functions
- Artificial Intelligence and Machine Learning
- Cloud Security
- PUBLIC POLICY and LAW, Cognitive Science, and Humanities
- Competency, knowledge, skills, task management based on interdisciplinary skills.
- Develop a partnership with industry, government, and universities.
- Establish a reliable student pipeline.
- Partnership for apprenticeships and cooperative education with industry and government agencies.
- PURPOSE: To influence policy decisions on shaping the information environment for operational and strategic/national goals.

FEDERAL PRIORITY FOR FUNDING: FRONTIER PROJECTS of National CAEs:

- Healthcare
- Modular Approach to CLOUD Security
- Encrypted Functions
- Artificial Intelligence and Machine Learning
- Cloud Security

- PUBLIC POLICY and LAW

PSU PARTNERS: ***(list of PSU Schools, Colleges, and Centers with faculty currently participating in the Cybersecurity Center)***

- College of Urban and Public Affairs
    - Mark O. Hatfield School of Government
        - Department of Public Administration
        - Department of Political Science
        - Department of Criminology and Criminal Justice
        - Center for Public Service
    - Department of International and Global Studies
- Maseeh College of Engineering & Computer Science
    - Department of Computer Science
    - Department of Engineering and Technology Management
- School of Business Administration
- College of Liberal Arts and Sciences
    - Russian Flagship Program
    - Department of Applied Linguistics
    - World Languages and Literature

Our task force of faculty met as two subcommittees, one for the undergraduate degree(s) and another for graduate degrees, as well as jointly and decided the following:

- As an NCAE-C in the state, PSU is uniquely situated to draft cyber studies degrees for our students. We believe that the least demanding path is for departments in respective colleges to prepare undergraduate and graduate certificates attached to students' majors, such as Cyber studies in WLL (Russian Flagship Program), Cyber studies in Political Science, and more. In some cases, these certificates could be minor. Also, we recommend looking into how this certificate can be used as "stacked up" degrees. The same also is desirable for graduate students.
- For example, the Computer Science Department already has a Graduate Certificate in Cybersecurity. This can be combined with a future Graduate Certificate in Public Policy (Hatfield School-Cup a) and result in a joint Master's Degree between MCEES and CUPA.
- Once these academic certificate programs draw new students, each department can expand their degrees to include a whole track in Cyber studies.
- We make all of these cyber studies certificates by making the four courses on Cybersecurity given to us by Professor Barbara Endicott-Popovsky as part of our N CA E-C partnership. These courses are 400-500 level classes and satisfy the Knowledge Units

K.U.U) required by the National Security Agency's NC AE-C standards. Thus, these courses make our tasks more manageable.

- Our partners at Chemeketa CC and Mt. Hood CC would like to see PSU develop an Applied B. S. Degree in Cybersecurity. They will then become a pipeline for CC students interested in a 4-year degree. This is a significant opportunity for PSU and ought to be pursued without hesitation. Otherwise, OSU will fill the need. We need to remember that OSU is applying to NSA, DHS for NCAE-C designation. 3 Community Colleges have a 2- year NC AE-C designations in Oregon: PCC, Chemeketa, and Mt. Hood.

NOTE: The highest priority of NSA is to see the creation of a sustainable pipeline for students (K 124) with a keen focus on equity, diversity, and inclusion.
PSU's connections to under-represented communities are our advantage in this regard. We must:

- 1. Reach out to Schools (K12) Oregon Department of Ed. told me that they could get us in touch with all the school districts to TRAIN TEACHERS in Cybersecurity
- 2. Sign partnerships with the three NCAE-C community colleges for a seamless transfer of students
- 3. Create non-credit workforce training certificates for private and public sector employees. This includes returning veterans. The Hatfield School established such a certificate and plans to launch it in January 2022.
- 4. Establish Cybersecurity Bootcamp. We decided that CyBint is an excellent company for our goals. NSA also recommends them. We are waiting for PSU's contracts to finalize the agreement.
- 5. As a result of our recent grant application to the NSA, we established good relations with vital private and public institutions.

We recommend signing MOUs with the key partners as soon as possible to expand research, education, and internship opportunities. Priority List:

INDUSTRY PARTNERS

- BPA
- PNNL
- PGE
- T Mobile
- Link Oregon G. Intel
- TAO
- Others TBD

ACADEMIC PARTNERS

- Oregon State University
- University of Oregon
- Chemeketa Community College (2-year CAE institution)
- Mt. Hood Community College (2-year CAE institution)
- Portland Community College (2-year CAE institution)
- NCAE universities and community colleges across the US.

FEDERAL INSTITUTIONAL PARTNERS

- National Security Agency
- Department of Homeland Security
- CISA
- US Cyber command

CONCLUSIONS

This analysis of Cybersecurity and cyber defense challenges and shortcomings facing the U.S. clearly shows a need for a new paradigm in addressing what needs to be done in educating our students and workforce training in this field. Existing overemphasis on technical education and training while ignoring the human factor in Cybersecurity misses the nature of the problem. Cybersecurity without the human element is meaningless. There is a growing gap between high-tech and policy/cognitive sciences. The lack of a bridge between the two makes the U.S. vulnerable to private and state attacks – in physical and informational social media. Therefore, while improving traditional academic studies in computer sciences, engineering, decision analysis, and public policy, we need to integrate our knowledge fields to provide interdisciplinary, holistic education and training. This requires a partnership at all levels: K-12, Community Colleges and Universities, government and, industry. **The Director of NCAE Programs Lynne Clark at NSA** recently emphasized that the new Strategic Planning 2022-2026 Plan's priority is to develop a competent, diverse workforce pipeline through a partnership of academia, government (including tribal governments), and industry in an applied learning environment. The Plan calls for regional internship programs, conducting regional exercises, expanded faculty development workshops, and K12-higher education networks. Few institutions around the country are talking about this need and initiating programs. Portland State is uniquely positioned to be at the forefront of this new paradigm because of its collaborative programs and visionary thinking tradition. Benefits include:

- Expand available research capabilities through public/private synergies.
- Cross-disciplinary education and training.
- Work on real-world applied research problems.
- Establish early connections with prospective employers and the emergent workforce.
- Competent and diverse pipeline for the workforce for government and industry.
- Contribute to sustainable regional economic development.
- Establish pipelines for students from High Schools and Community Colleges (especially the CAE institutions such as PCC, Mt. Hood CC, and Chemeketa CC) to attain advanced degrees in Cyber studies.

To move PSU into the forefront of developments in cybersecurity education, research, and workforce training, we ought to focus on how to capitalize on initiatives that capture NSA-DHS-NSF priorities in this field:

1. Sustainable K12-Community College-University pipeline of students interested in Cyber studies to meet national workforce needs in the private and public sectors, attract underserved and underrepresented communities to this field and promote diversity and inclusion not only in STEM but in Cyber studies (interdisciplinary).
2. We need to join a coalition of other NCAE-C institutions in areas of interest for PSU for student and faculty training.
    a. Look into the K-12 pipeline grants. And bring the Oregon Department of Education into the discussion. NICE curriculum guidelines and CAE Knowledge Units K.U.U) comprise the foundational base of such programs.
    b. Train the trainers' program for communities (for example, in underrepresented communities). The University of Louisville has a program administered by Professor Sharon Kerrick that could be a good partnership. Another partner of the program is Professor Drew Hamilton at Mississippi State University.
    c. The K12 program also evolved within the NCAE-C community to develop an education program of 60 hours, eight modules, interactive training through the Moraine Valley Community College (Professor John Sands and Professor Jesse Hairson at the University of Alabama Huntsville). The NCAE K12 Regions Investing in the Next Generation (RING) project, led by the University of Alabama in Huntsville (UAH) and Moraine Valley Community College (MVCC), was established in FY20 to provide a comprehensive program designed to engage and develop middle and high school students in a year-round cybersecurity education program. RING will launch the project's infrastructure, create a curriculum, a national directory of CAE K12 pipeline programs sponsored by individual institutions, educational games, and other after-school and extracurricular activities. The ultimate objective is to inspire students to a

cybersecurity career, prepare them for post-secondary education in Cybersecurity, and make educational resources available to schools. Target audiences are home-schooled, rural, and under-represented students.

3. CYBER CORPS: Scholarships for Service through NSF. PSU should seriously look into this for opportunities for our students. The Scholarship for Service (SFS) program is administered and funded by the National Science Foundation (NSF) in cooperation with the U.S. Office of Personnel Management (OPM). Scholarship benefits include full tuition and fees, a cost-of-living stipend, travel expenses, and professional development reimbursement. Students awarded a scholarship incur a service obligation to the government upon graduation from UAH and must participate in a paid internship during the summer semester.
4. The SFS shares an application with the Department of Defense (DoD) Cyber Scholarship Program (CySP). The CySP has similar benefits to the SFS; however, students are immediately paired with a DoD employer upon receiving the scholarship. Applicants are considered for both scholarships under a single submission.
5. Promote interdisciplinary education and research at PSU, focusing on local/regional cybersecurity vulnerabilities (see discussion above on threats).