Cyber Public Private Partnership ICS/SCADA and Critical Infrastructure Protection Strategic Vision

Col. Scott Nelson

Dr. Barbara Endicott-Popovsky

EXECUTIVE SUMMARY

Since 2003 cyberspace has become a significant national asset for the United States and our elements of national power: Diplomacy, Informational, Military and Economic (DIME). The global balance of power is now shaped by a new multi-polar diffusion of power, disruptive technologies and Moore's law of technology advancement [1]. These factors have enabled cyberspace Advanced Persistent Threats (APT) which include; criminal networks, nation states, terrorist organizations and others, to develop leveling strategies against the United States national strengths; however, early in the Internet's development the focus was on access and ease of connection, not security. Cyberspace today now hosts and underwrites the global economic market worth trillions of dollars. The United States is critically unprepared for a massive disruption of our critical infrastructure from a cyberattack. APTs (Nation states and non-state actors) have identified and continue to map critical vulnerabilities in each of our national critical infrastructure sectors: chemical, communications, commercial facilities, critical manufacturing, dams, energy, defense industrial base, emergency services, financial, food and agriculture, healthcare and public health, nuclear (reactors, materials and waste), transportation, water and waste water systems, information technology, and government facilities--and have demonstrated intent and capability to disrupt them in case of an international conflict or crisis. The nation lacks a comprehensive and executable strategy to effectively respond [2] Several major factors contribute the

nation's unpreparedness. For one, the nation is critically short of cyber security professionals to meet the demand for national cyber defense. For another, Federal government agencies and US policy/laws inadequately prepare, coordinate, share and integrate public and private capabilities to defend the U.S. from a massive cyber disruption. There are more…

Focusing on the first issue, the Department of Defense has identified a critical shortage of cyber security professionals in a number of reports, including, GAO [1] and RAND [2]. The Reserve component was identified as a potential and immediate possibility to lessen the shortage of cyber security/defense professionals. The US Army Reserve (USAR) stands at the threshold of providing significant and critical need to the Federal government, DoD, public and private sector through its new P3i program. This program is designed to understand, identify and fill a strategic opportunity for the USAR to provide an expandable and tailored solution for bridging the civilian and military, cyber security talent gap. Development of a successful USAR Cyber pipeline requires a comprehensive program that starts with our academic partners to build cyber security educational opportunities, as well as develop civilian cyber employment opportunities to maintain skills, maintain relevance and recruit/retain the force and finally a shaping force that contributes to developing a generating force. Toward this end, it is recommended that the DOE Hazardous Materials Management and Emergency Response (HAMMER) Federal Training Center be utilized as the initial cyber security training facility due to its capabilities to bring together Federal, military, and civilian personnel.

CONCLUSIONS / RECOMMENDATIONS

1) The US has an urgent need for an increased number of cyber security experts to protect the US cyberspace from nefarious attacks from foreign nations, terrorist groups, and private hackers.

2) The US needs more centers of academic excellence (CAEs) for providing advanced cyber security education and training to fill the current short fall in the government, military, and private sectors.[1]

3) The DOE HAMMER Federal Training Center is recommended to be the initial advanced cyber security training facility. The training program will be under the direction of, and shall be a partnership of, public and private cyber security experts.

4) As the program develops, it is expected to be a model for other centers of excellence for advanced cyber security to be established at other locations to be determined.

BACKGROUND

The threats from cyberspace to our nation are significant. The Director of the National Intelligence, James Clapper, in recent Congressional testimony on the 2013 National Intelligence Estimate (NIE) stated his concern for the defense of the nation from cyber threats. "When it comes to the distinct threat areas, our statement this year leads with cyber and it's hard to overemphasize its significance." [3] The NIE report goes on to warn that we should prepare for increasingly destructive attacks that are designed to render systems inoperable, or could delete critical information, as advanced malware and techniques continue to evolve and proliferate, citing the following 2013 examples:

- In March 2013, South Korea suffered a sizable cyber attack against its commercial and media networks, damaging tens of thousands of computer workstations. The attack also disrupted online banking and automated teller machine services [4].

[1] 200+ DHS/NSA Centers of Academic Excellence exist across the United States at various colleges and universities, mostly concentrated around the Beltway, the East Coast seaboard through Texas. While these have been engines of dissemination for emerging government standards for cybersecurity education and workforce development (NIST/NICE initiative), there are thousands of universities and colleges that are not aboard and are graduating students with an unawareness of cybersecurity.

- Although likely unrelated to the 2012 network attack against Saudi Aramco, these attacks illustrate an alarming trend in mass data-deletion and system-damaging attacks [5].

Cyber threats could be anything that leads to interruption, meddling or destruction of any valuable service, function or item existing in critical information systems/networks [6]. Whether of "human" or "nonhuman" origin, the threat analysis must scrutinize each element that may bring about conceivable security risk [7]. Cyber threats take many forms from denial-of-service attacks, to beckoning malware, and root access. Today, the actions of nation states, non-state actors, criminal networks, hackivists and terrorist networks are so concerning that the Director of the National Security Agency (NSA) worries that cyber attacks could shut down U.S. critical infrastructure [8]. This could occur for a number of different reasons. For one, nation states see cyberspace capabilities as an asymmetric capability that can level the playing field with a superior economic, diplomatic and military foe like the United States. As early as 1999, Chinese military strategists were envisioning a weaponization of cyberspace as a deterrent to the United States' massive military superiority.

The new trend to create efficiencies and manage economies of scale for the nation's critical infrastructure by leveraging online capabilities is a potential Achilles heel and creates a significant vulnerability. The cyber-physical systems that manage critical infrastructures, called Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition systems (SCADA), run most of the nation's critical infrastructure.

One potential solution to lessen this looming national crisis is to focus the US military's Reserve Component (RC) on the cyber defense mission for the homeland. The Department of Defense can integrate the RC cyber forces to significantly contribute to the defense of national critical infrastructure, provide a partial solution to the massive shortage of cyber security professionals and bridge the information divide between the military, intelligence community, government agencies at the Federal, state and local levels and private industry. Industry is unprepared for seeing itself as a military target. The enemy is too well aware that

the United States could be crippled with attacks on the private sector, which owns most of critical infrastructure such as the electric grid and water systems.

Development of a successful USAR Cyber pipeline requires a comprehensive program that starts with our academic partners to build cyber security educational opportunities. This combined with civilian cyber employment opportunities to maintain skills, maintain relevance and recruit/retain the force will lead to shaping a force that contributes to developing a generating force. In order to achieve this goal, an initial training facility must be established. Unfortunately, the current DoD and Army school systems do not yet provide the throughput or advanced skills required for the RC. Thus, it is recommended that the DOE HAMMER Federal Training Center in Richland, Washington be utilized as the initial cyber security training facility due to its capabilities to bring together Federal, military, and civilian personnel in a myriad of programs. HAMMER collaborates with the Pacific Northwest National Laboratory (PNNL) and Washington State University which has a branch campus in Richland. We are suggesting that the collaboration be enlarged to include the University of Washington, an NSA/DHS CAE in cybersecurity education and research and the community college system that is emerging as a network of 2Yr-CAE's.

DISCUSSION

Two senior Chinese People Liberation Army Air Force Colonels published "Unrestricted Warfare" describing a new style of economic, psychological, media and cyber warfare against superior adversary forces, economies and populations [9]. Some reports place the PLA investment in cyberspace operations at 130,000 personnel, more than eighteen times greater than the combined US militaries cyber mission force [10]. Russia has already significantly demonstrated its military cyber power in the conflicts in Estonia, Georgia and Ukraine. In cooperation with the Russian Business Network, the Russian government has generated significant damage to US companies and possesses an advanced, and very sophisticated, cyber attack / exploitation capability. The militarization of cyberspace as a war fighting domain is done. The problem for the United States is that entry into the cyberspace arms race is a low cost, easy and an effective leveler for much smaller, or

economically inferior, determined adversaries. The emergence of capabilities such as STUXNET that can effectively destroy physical infrastructure/systems through advanced malware is a disturbing trend for the nation's critical infrastructure. Countries like Syria, Iran, North Korea and terrorist organizations have already proven their cyberattack ability by disrupting US national security targets, businesses and our allies/interests abroad.

Cyberspace enables the United States to run the country and connect multiple infrastructures into a functioning system of systems. This trend will continue as cyberspace expands to the 'internet of things" and integrates cyber-physical systems. These systems, ICS and SCADA, now run most of the nation's critical infrastructure. Unfortunately, we have created serious attack vectors that require only minimal investment and virtual presence to exercise. The homeland is now no longer immune, protected by two oceans and cooperative countries on all sides. We have opened the homeland to ill-intended adversaries that see our country as the enemy. We have given them the tools to penetrate to our core capabilities.

To elaborate, as computers matured over the last 50 years, ICS/SCADA systems have become more networked and integrated into the controls of almost all of the nation's critical infrastructures. For example, ICS systems control execution of concurrent instructions to process controls in refineries, programmed logic controls on the manufacturing floor or Master Terminal Unit (MTU)/Remote Terminal Unit (RTU) in widely distributed SCADA systems that control essential systems such as pipelines, electrical grids and sewage systems [11]. These systems include monolithic (and some of the oldest) standalone, distributed, and networked systems and is about to control the emerging internet of things that will run everything from our households to our cars [12]. Adding to the challenge, these systems of hardware, software, firmware and physical controls blend all generations of systems, making mitigating risks challenging [13]. This is why STUXNET, the advanced malware that attacked the Iranian nuclear centrifuges, is so disturbing to critical infrastructure managers, because many of the vulnerabilities in these systems are not known. They were never designed to withstand attacks in an interconnected world. The engineering emphasis was on safety, not security: two different, although

overlapping in some cases, sets of requirements. Additionally, the balance in the private sector between the cost of security versus the bottom line can be challenging. Using the US Army as an example, it has thousands of these systems running everything from garrison sewage, pipelines, power grids, and security systems to weapons system production lines. Those developing and managing these systems have limited knowledge of an ICS/SCADA asset inventory, let alone which systems are networked, connected to the Internet and therefore vulnerable to cyberattack. Critical infrastructure is also effected by policy decisions that impact the maintenance, upkeep, funding and security considerations for much of our publically or government (local, state, federal) controlled ICS/SCADA. The list goes on. We are going through a massive paradigm shift with the information age driving inexorably forward. As a society, this has tested our collective imaginations to understand the unintended consequences like these just described. It makes us vulnerable and hands opportunity to adversaries.

Why is it so hard to defend the nation's critical infrastructure from cyber attack? The management of critical infrastructure has significantly changed over the last 30 years from two thirds publically owned and operated to now two thirds privately owned [14]. This provides some significant challenges in comprehensive cyber security and critical infrastructure protection including legal constraints (the public and private sectors are walled off by legal and regulatory boundaries making cross-sector collaboration on something like a cyberattack challenging), privacy concerns (what are local governments going to do with massive amounts of personal data they collect for everything from taxes to utility bills. Do they understand the privacy and security implications and responsibilities), limited budgets and shortage of personnel (The private sector is prone to see defending against nation state attacks as a Federal government responsibility. Further, they are wedged between profit/loss concerns and rate-payers allergies to increased utility rates).

One major problem for the private sector, like it is for the public sector, is the shortage of qualified and experienced cyber security professionals and their salaries. Both RAND and the Government Accounting Office (GAO) have identified the lack of cyber security professionals in the government and private sector as critical

vulnerabilities that need shoring up to achieve the nation's cyber defense [15]. Recent reports have identified shortages of thirty to forty thousand cyber security professionals in the Federal government alone [16]. Further exacerbating the problem, while the government and private sectors have both identified cyber security as a significant threat, they remain far apart on how to act, who acts and when to act. Policy, law and funding inaction from the President and Congress on down have retarded a comprehensive cyber strategy and hurt the Federal government's credibility when it comes to directing cyber defense. (A much need Cyber Security bill has been stalled in Congress for over a year.) Finally, cyberattack information sharing between the public and private sectors has improved but remains critically inadequate in proactively providing assistance for companies under assault.

The US military's Reserve Component (RC) can be a major contributor to the Services and Joint Forces as cyber operators and defenders in the near future. However, successful long term RC cyber support to the Joint Force requires 1) development of an RC Cyber Soldier pipeline for recruiting new/current RC soldiers and transition for the AC (active component) Soldiers, 2) training/education, employment in the cybersecurity profession, and 3) education-training with research infrastructure (TRAIN AS YOU FIGHT). To address this need, the DoD RC Cyber Private Public Partnership was initiated in support of the Chief of the Army Reserve's Private-Public Partnership program (P3). The program is designed to emphasize the professional development, recruiting and retention of cybersecurity talent in the RC. The Cyber P3 lines of effort (LOEs) are nested within USCYBERCOM Commander's strategic vision.

The US relies on information systems and data at every level of national power. US critical infrastructure and military operations are specifically at risk from Advanced Persistent Threats (nation-states, non- state actors, terrorists and criminal networks). The nature of cyber defense has shifted from passive defense (reliance on defense-in-depth and firewalls) to active defense, with an emphasis on highly skilled and critical thinking cyber professionals. It's no longer a matter of if the adversary gets inside our defenses, but when. The probability is 1 [17]. The demand

for these individuals far outpaces the Cyber Soldier and unit inventory. The current DoD and Service school systems do not yet provide the throughput or cybersecurity advanced skills required for the RC.

Given that the RC does not have the resources currently, then civilian opportunities (universities and colleges) are the more likely choice for developing and maintaining cyber skills, maintaining continuous skill relevance, recruiting/retaining the right cyberforce, and ultimately a shaping force that contributes to developing a generating force. In order to achieve the latter, an initial training facility must be established very soon. The DoD and Services lack a Cyber Critical Infrastructure advanced training center to develop ICS/SCADA and CI-KR related cyber skills (individual and team-focused). Thus, it is recommended that the DOE HAMMER Federal Training Center in Richland, Washington be utilized as the initial cyber security training facility due to its capabilities to bring together Federal, military, and civilian personnel in a myriad of programs. HAMMER collaborates with the Pacific Northwest National Laboratory (PNNL) and currently conducts military and International Border Security Training (IBST). PNNL, operated by Battelle Memorial Institute's Environmental Molecular Sciences Laboratory (EMSL) is a national scientific user facility located at the PNNL campus in Richland, Washington. EMSL provides experimental and computational resources to address environmental molecular science challenges which have been accelerated when combined with leading-edge hardware, efficient parallel software, accurate and predictive theories and visualization capabilities.

PROGRAM PURPOSE

Current plans underway address organization, training and education and integration with the Army Reserve Component (Army National Guard and US Army Reserve) into the national defense strategy for cyber defense of critical infrastructure. DoD has organized the military cyber force into three strategic echelons with approximately 6000 military cyber personnel and 141 cyber teams [17]. These echelons are the National Mission Force focused on cyber operations outside the US, the Component Commander Support Force focused on support to the six Geographic Combatant Commanders, and the Service support teams focused

on providing direct cyber defense support to their Services' (Army, Air Force, Navy, Marines) strategic information systems. None of these forces is focused on employing capabilities beyond the responsibilities of the DoD. The Department of Homeland Security (DHS) is the Federal government's lead agency for defense of critical infrastructure (CI), but they realize that a whole of government approach will be required to proactively respond to CI cyber defense. One way to shore up DHS capabilities is integrating the Army's Reserve Components into DHS and the states' emerging CI cyber defense strategy. Another is to jointly include DOE where their cyber-experience can help both DoD and DHS. Currently, the ARNG and USAR have been directed to stand up twenty-one 39-Soldier Cyber Protection teams (CPT). The CPT has five 7-Soldier sub-teams that are trained to perform missions such as cyber training, policy reviews, penetration testing, counter intrusion, forensics, and vulnerability assessment. These teams are designed to be directly linked to the national intelligence community for integrating real time cyber threat intelligence into the team's operations. The CPTs conduct both routine and crisis response operations to support Cyber Defense Service Providers (CND-SP). The CND-SP in critical infrastructure is similar to the network defense teams supporting ICS/SCADA systems. None of these RC CPTs have been applied to a mission by Army Cyber Command or US Cyber Command. The RC could be integrated in the critical infrastructure cyber defense system through mission requests by DHS, via the 10 FEMA regions, to the DoD. Under similar circumstances, DOE has eight National Laboratories which have excellent experience with computer programs and cyber communications. DOE, together with DoD and DHS, may finally have the knowledge and support to approach a national defense strategy to combat the cyber problems we face as a nation.

Nevertheless, for a successful program it is critical to integrate these RC CPTs prior to crisis so they can identify and understand key cyber terrain (essential hardware, software and cyber-physical systems), train to mission requirements, but more importantly, build relationships with supported public or private critical infrastructure providers. This could be done through deliberate vulnerability assessments partnered with the CI provider or through realistic exercises. Training and education is critical to the CPT success at the individual and team level. The

power of the RC is in having civilian-acquired skills linked with military skills that serve dual use in reservists' civilian and military professions. An analog is reserve component doctors and nurses who quickly integrate their extensive medical practice knowledge, skills and attributes when needed by the Army. Another opportunity to demonstrate the value of reservist cyber defense skills is building Cyber public-private partnerships. Army cyber training programs are emerging, but even at maturity would require civilian and academia's assistance to maintain continuous improvement in the CPT soldiers' skills, knowledge, experience and expertise, especially the unique skills needed to defend ICS/SCADA systems.

The development of a public-private partnership would serve all parties by enhancing skills of reserve military personnel, providing a pool of military and university trained and educated cyber professionals available for civilian employment and who provide a catalyst for holistic cyber defense support to the nation's critical infrastructure. In essence, building a cyber defender stool with three supporting legs: the military trained and skilled reserve career directly linked to fulltime civilian cyber professions, aided by continuous education opportunities provided by universities. Additionally, cyber defense training infrastructure is critical to exercise and validate skills, and generate experience and critical multi-agency relationships. Cyber defense in particular is a profession learned by doing, similar to learning a language. Cyber defense critical thinking skills are best developed and tested through immersion in realistic cyber exercise and scenarios. The military motto "train as you fight" fits for cyber defenders. In theory, much of the critical infrastructure exists today in a simulation form with some modifications. This is why we propose, as a potentially viable solution in Washington State, the 88-acre HAMMER facility and its physical training infrastructure. This Federal training facility has numerous critical infrastructure systems replicated and provides a natural location for establishing a closed cyber ICS/SCADA range. In partnership with State's university structure (Washington State University, the University of Washington) and DOE, DHS, Federal intelligence agencies, the State of Washington, US Army Reserves, the WA National Guard, and other industry partners, HAMMER could provide the physical link missing from experimental ranges to help identify, replicate, research, understand and defend against cyber

threats to critical infrastructure. The universities could serve as the virtual research cyber range backbone supported by public and private partners.

Missing in Washington State is the physical infrastructure to demonstrate and train against the effects of a cyber attack against cyber-physical systems in a collaborative environment where all partners can research, test, train and work toward cyber resilient networks, systems and people. This concept could fill the void and provide platforms for multiple partners from military, DHS, DOE, law enforcement, state, local and private industry partners to train and exercise together. Additionally, the training partnership could provide a solution to another identified problem which is information sharing. The Federal government generally has access to most of the critical threat information that describes threat intent, capabilities, access points and vectors employed by our cyber adversaries. The reserve CPTs, with additional reserve intelligence capabilities, could serve as a natural link between the intelligence community and state emergency operations or cyber defense centers. Across the country, state threat fusion centers that integrate emergency managers, policy makers, law enforcement, Federal representatives (DHS/FBI) and the military provide opportunities to strengthen information sharing up and down the system about cyber threat and events in real time. Finally, the RC also provides an operational bench of cyber warriors and RC cyber units to retain the Army's expensive investment in ready-trained AC cyber warriors as they transition from active duty. These AC cyber soldiers can also serve as capable civilian employees. With future demand for these RC cyber soldiers and units far outpaces the current inventory, we are providing a national service by creating and nurturing this talent pool of prepared cyber warriors.

Cyber threats to ICS/SCADA and emerging SMART GRID capabilities are a direct threat to national security and the economic well-being of the United States and its allies/partners. The SCADA problem transcends all government agencies (Federal/state/local and tribal), academia and industry. Military reserve components can contribute significantly to the defense of national critical infrastructure, provide a partial solution to the massive shortage of cyber security professionals and bridge the information divide between the military, intelligence community, government

agencies at the Federal, state and local levels, and private industry. The HAMMER model provides a useful concept for further strengthening multiple agency response to cyber defense of CI. The ARNG and USAR stands at the threshold of providing significant and critical support to the Federal government, DoD, and the public and private sectors. Cyberspace has become weaponized and the Army must be prepared to operate, defend and maneuver in Cyberspace. The Army should expand, mission, and integrate the ARNG and USAR twenty one CPTs and existing operational cyber capabilities to serve as an immediate surge capability to support national cyber protection of CI.

PROGRAM OBJECTIVES

The Cyber Private Public Partnership is intended to provide a catalyst for building cyber security professionals in the USAR. The Cyber P3 initiative targets: future recruits, initial entry soldiers, transitioning AC soldiers to RC, prior service entering the RC, existing RC soldiers in cyber-related fields and existing professional, cyber-soldiers. The program directly supports the recruiting, retention, transition and cyber skill progression of RC Cyber soldiers across the RC (Support, Training, Operational and Functional Commands). Finally, the program is designed to provide a pool (individuals, units and leaders) of exceptionally qualified and experienced cyber soldiers that can support service, joint and interagency cyber events and operations. The aim is to bridge the civilian-military divide with mutually supporting careers and professional opportunities in cyber security. The program is designed for 3500 - 5000 Army Reserve soldiers and an equal number in the other Service Reserve Components and National Guard.

Cyber security response is best when it is active and proactive versus passive and reactive. The US relies on information systems and data for almost every level of national power. US critical infrastructure and military operations are specifically at risk from Advanced Persistent Threats (nation-states, non- state actors, terrorists and criminal networks). The nature of cyber defense has shifted from passive defense, reliant on defense in depth and firewalls, to active defense, with an emphasis on highly skilled cyber professionals who are critical thinkers. The Reserve Component (RC) in a number of reports including GAO [18] and RAND [19]

was identified as a potential and immediate possibility to lessen the shortage of cyber security/defense professionals.

The general threats to our national critical infrastructure can become a system forming factor to help define a model using the U.S. military's reserve component cyber forces to prepare, plan, coordinate, respond, mitigate and recover from a significant cyber attack on the US.

TABLE OF STATE BY STATE CYBERSECURITY CAPABILITIES

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
AL	Standard. Main cybersecurity page for the state: http://www.cybersecurity.alabama.gov/ State Information Security Policy: http://cybersecurity.alabama.gov/ documents/Policy_600_Information_ Security.pdf	Seven NSA/DHS-designated Centers of Academic Excellence	Nine universities offer various degrees	Five research centers at universities	A number of government contractors. Companies: Northrop Grumman, Quantum Research, Boeing, Booz Allen Hamilton, Radiance Technologies	Three CAEs have received SFS grants	Good
AK	Standard/Needs improvement. Alaska's DoA Security website, with links: http://doa.alaska.gov/ets/security/ The State of Alaska was fined $1.7 million for a security breach in 2012: http://www.securitymagazine.com/articles/83272-state-of-alaska-fined--1-7-million-for-security-breach-	One	One university and one college	One	Siemens General Dynamics – IT, AT&T	None found	Low
AZ	Law/policy-wise we couldn't find much. There does not appear to be any state-level cybersecurity policy websites for Arizona.	Three	Three universities offer various degrees	Three	Arizona is growing a "Cybersecurity Valley" with a number of private security companies as well as government contractors who are researching cyber security: Honeywell, Mitre Corporation, Raytheon, General Dynamics C4 Systems, Booz Allen Hamilton, etc.	Two CAEs have received SFS grants. Other NSF grants have also been awarded to University of Arizona, including the AZSecurity Cybersecurity Fellowship program.	Rather good, though can be even better.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
AR	The AR state government seems to promote cybersecurity transparency and education online more than some others. The state government promotes cybersecurity awareness through their sites and observing events such as "National Preparedness Month." Arkansas State Department of Information Systems (DIS) Cyber Security site: http://www.dis.arkansas.gov/security/Pages/default.aspx Arkansas Department of Education Cyber Safety Resources site: http://www.arkansased.org/divisions/learning-services/technology-initiatives-and-resources/cyber-safety-resources	Two	Two universities and one college	Two	Not very many security companies here: AT&T, General Dynamics – IT, etc.	None found	Underdeveloped, though the state government makes an effort.
CA	California envisions their state as a leader in cybersecurity innovation. The state has a robust legislative framework related to information security with some of the earliest data breach laws on the books. The state government engages in cyber awareness exercises and has a cross-sector cybersecurity working group focused on improving the state's posture against security threats and vulnerabilities.	Eight	California has an enormous academic infrastructure with well over a dozen programs tailored towards cybersecurity education in a number of narrowed specialties.	Home to multiple cybersecurity focused research and development centers.	Home not only to the major Silicon Valley companies but also hundreds of small start-ups, niche market companies, and boutique firms providing cybersecurity services.	University funding coming from NSF, DoD, DoE, and other. Grants from cash flushed tech companies / silicon valley firms.	Very good

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
CO	Colorado Office of Information Security (OIS) http://www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1249667675596 The Colorado Office of Information Security is a unit within the Governor's Office of Information Technology and is the single state source for cyber security readiness and awareness. OIS is directly aligned with the goals and objectives of the National Strategy to Secure Cyberspace. Working closely with federal, state, local and private sector partners, the Office of Information Security actively gathers and analyzes information on cyber threats and vulnerabilities that present risk to the state's information systems or the critical information managed within. State Information Security Policies http://www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1251575408771	Five	Offers a number of offline/online degree programs with focus in cybersecurity through six universities.	Four major centers	A large number of contractors and military presence focusing on cyber security in Colorado, including the Air Force Academy and their associated cyber research center. Colorado Springs was named one of the "Top 5 Cities for Cyber Security Jobs" by clearancejobs.com. Companies include: Northrop Grumman, Lockheed Martin, CenturyLink, Booz Allen Hamilton, Raytheon, etc.	1.25 Million AFOSR equipment grant given to UC Colorado Springs for the Cyber Research Facility	Good
CT	The first state to present a unified cyber security utilities response plan with the Public Utilities Regulatory Authority (PURA). They are working to integrate their activities with DHS. The state has a Cyber security resource page Welcome to CT.Gov/Cybersafe and passed a cyber-bullying law in 2013.	One	7 universities & 3 colleges	Two	UCONN Tech Park $162.3 million investment. state-of-the-art facility for advancing the competitiveness of Connecticut industry, and for the economic success of the state: Comcast, Pratt & Whitney, Hartman International, etc.	A cybersecurity research program underwritten by Comcast (Millions of $$ over three years). DoD - $75 million? $2 million in Fed grants (2012) NCAEIAR	Rather good, though can be even better.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
DC	Evidence shows that the DC metro area is being "remade into the federal government's hub for cybersecurity work." Statistics show DC as having the most cybersecurity job listings in the country.	Five	Virtually all of the academic institutions in DC (at least, five) now offer cybersecurity-related curricula.	Four	DC is fast becoming a hot bed of cybersecurity jobs, most notably, of course, is the federal government and the military; Northrop Grumman, Booz Allen Hamilton, General Dynamics – IT, etc.	One CAE has an SFS scholarship	Good
DE	Delaware is extremely proactive in how it manages and cultivates cybersecurity. There are multiple broad collaborative efforts in progress that will increase the state's ability to secure not only its own assets but to provide talented young cybersecurity professionals to the federal government. Delaware is also one of a number of states to leverage the capabilities of the state's National Guard for cybersecurity.	One	Two universities & two colleges	Delaware lacks the research facility footprint found in many larger states.	The state's cyber efforts are heavily oriented towards intellectual property protection and focused on corporate cyber security: JP Morgan Chase, DuPont, Northrup Grumman, PricewaterhouseCoopers	Regional Cybersecurity Initiative funded by half million dollar NSF grant	Can be much better
FL	Florida recently repealed its security breach law and passed "sweeping legislation" seen as possibly the broadest in the country. The state marked $5 million of their 2015 budget to fund a new state-wide Center for Cyber security. Aim is for Florida to develop cybersecurity as a central pillar of its economic future.	Seven	At least, 15 colleges/universities offering cybersecurity and/or information assurance-focused curricula.	Four	Most of the cyber jobs in FL seem to be with government contractors: BAE, Lockheed Martin, Northrop Grumman, etc.	Four NSF grants	Good

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
GA	The state government does not appear to have an office/agency dedicated to security, nor is there a public website providing information on cybersecurity.	Five	Six universities granting cyber security degrees.	Five	Companies: Damballa Labs, Gyrus, Purewire, Dell, Siemens, PwC, Lockheed Martin, Apple, etc.	$10 million DHS project investigating open source, being led by Georgia Tech. One CAE has an SFS scholarship	Rather good, though can be better.
HI	The Hawaiian governor recently appointed a Chief adviser for Technology and Cybersecurity in a move to tighten ties with the federal government and build Hawaii's cybersecurity profile. Recent legislature and state government organizations focus on cyber-crime, cyber bullying/stalking and exploitation of children.	One	Two universities & one college	Four	Booz Allen	The University of Hawaii – West O'ahu received a $245,000 grant from the Office of Naval Research to establish a STEM Center of Excellence at the University.	Can be better
ID	Idaho state government has a cybersecurity awareness website that provides useful links and information for home users, tens, kids, businesses, and educators.	Two	Two universities	Two	Companies: McAfee, CenturyLink, etc.	Two CAEs have SFS scholarships	Can be better

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
IL	The governor's office is taking a proactive approach to linking state policy with the development of cyber awareness and building awareness of cybersecurity career fields through well-spaced public relations announcements, attracting veterans into the career field and free on-line competitions through cyber aces and Illinois' CAE2Y. The state proudly displays their involvement in the MSIAS.	Eight	Seven universities & one college	Argonne National Labs: Argonne maintains four laboratory sites - Lemont, Carbondale, Chicago and Champlaign,	Companies: BAE Systems Applied Intelligence, Boeing, Booz Allen Hamilton, Deloitte, IBM, KPMG, Lockheed Martin, Northrop Grumman, PwC, Verizon, etc.	In 2010 Illinois received a $1million grant to develop cybersecurity first responded training to be rolled out nationally.	Very good
IN	Indiana has well defined cybersecurity laws and policy. The Universities drive cyber activities within the state, as does the government sector.	Three	Two universities and one college	Four	Companies: Boeing, IBM, PwC, etc.	No data	Can be better
IA	The state has a slow posture regarding cybersecurity laws and government activity. Iowa became only the 43rd state to enact data breach notifications laws.	One	Three universities & one college	Two	Research parks at universities have: BASF, Siemens, etc.	One SFS grant	Can be better

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
KS	The state legislation (Chapter 50, Article 7a) specifically addresses issue of Information Security (Cybersecurity) which includes protection of consumer information.	Four	Three universities & one college	One	Companies: HP, etc.	One SFS grant	Can be better
KY	Kentucky is a latecomer to the field in cybersecurity. In 2012, the state finance cabinet posted social security numbers on their website. Recently Kentucky passed two bills which now require local government agencies notify people within 35 days of PII being mishandled or stolen. Kentucky is only the 47th state in the union to pass cybersecurity laws.	Kentucky is one of 7 states without a CAE institution.	Two universities	Nothing found	A bright spot in Kentucky is the job market, possibly because the businesses are trying to come up to speed with the rest of the pack. Companies: Time Warner Cable, Kforce, etc.	Nothing found	Low
LA	Legislation Act 772 – 2001 regulates all Information Technology related policies. This includes IT Governance, Security Policies, Computer Infrastructure and General Policies. This has been revised with few additions (La. Rev. Stat. § 51:3071 et seq. (Acts 2005, No. 499, §1, eff. Jan. 1, 2006.))	Three	Three universities & one college	Four	Companies: IBM, etc.	Nothing found	Can be better

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
ME	Maine does not have a generally high level of cybersecurity activity, but the state has the requisite data breach laws and a relatively active state government offering information and participating in some conferences targeting IA/CD. The research and education capacity of the state is rather small.	None yet, but the NSA and DHS are designating the seven-school system a National CAE in IA and Cyber security: http://www.pressherald.com/2014/11/21/maine-universities-recognized-for-cybersecurity-education/	Two universities	Two	There is about 900 job offers in information security field in Maine according to Indeed: http://www.indeed.com/q-Information-Security-l-Maine-jobs.html	$1 million in grants from the National Science Foundation and Maine Technology Institute to design and build cyber security lab at USM.	Needs serious improvement, and there are good efforts to achieve that.
MD	Tons of state backing. Examples: Implementation of a cyber investment tax credit for companies as an incentive. Creation of a Commission on Cybersecurity Innovation and Excellence. Creation of a Resource Center for Cybersecurity (co-led by Maryland and Michigan). Creation of a Baltimore / Washington task force to implement a strategy for cyber around CYBERCOM activities. Creation of a Director of Cyber Development.	16	16 universities, colleges or tech institutes that offer degrees or certificates in cyber.	Six. Also, nearby federal agencies and institutions offer a significant strategic advantage. For example, they are located by: NIST, CYBERCOM, NSA/CSS, NASA High Performance Computing Center-2: schedule for completion in 2016 to be located at Ft. Meade.	Venture Capital Deals: 374 from 2008-2012 in cybersecurity valued at $2,096,999.000. There are over 75,000 employed in Cyber Security-related jobs in the Greater Baltimore/Central Maryland region. In addition, there are nearly 20,000 open Cyber Security job positions in Maryland. There are currently more than 11,000 companies in Maryland that create products and services to protect against cyber-attacks, including heavy hitters such as Northrop Grumman, JHU APL, Verizon, Lockheed, Booz Allen, SAIC, and CSC.	TEDCO fund invests in start-up cyber security technologies for Maryland based companies with more than 16 full-time employees and less than $500,000 in outside investments. Investments per company will not exceed $100,000.	Excellent

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
MA	Should likely be considered as one of the model states regarding IA/CD capability. The state has standard cybersecurity, cyberbullying, and identity theft laws and a fairly active state government that recognizes and supports the advancement of cybersecurity as a strategic need. The state is one of six in the US that has developed and utilizes the Cyber Aces (http://www.cyberaces.org/) program. The program is a cybersecurity talent development effort using competitions to select promising students for cybersecurity education and internship opportunities.	Four: Boston University, Northeastern University, Worcester Polytechnic University, and University of Massachusetts – Amherst. Additionally, Massachusetts is home to two of the nation's most prestigious and technically advanced universities: Harvard and MIT.	The following institutions offering varying cybersecurity degree options: Bay Path University, Boston University, Worcester Polytechnic, University of Massachusetts, Northeastern University, Mass Bay Community College, Brandeis, and many affiliate universities in the University of Massachusetts system.	The state is home to two major cybersecurity research organizations with the MITRE Corporation's Bedford location and Lincoln Labs at MIT. There are many other smaller centers, organizations, and working groups operating in both industry and academia.	The state has companies with cybersecurity missions in all the major sectors like finance, defense, tech, government, healthcare, and energy, including: Akamai Facebook, Liberty Mutual Group, Pfizer Inc., etc.	The academic institutions are massively funded through federal grants.	Good
MI	Michigan has a long standing tradition of building and maintaining collaborative internet/security relationships. The legislature passed three cybersecurity laws, Identity Theft Protection Act 452, Social Security Number Privacy Act and the Michigan Anti-spam laws.	Five: Davenport University, Eastern Michigan University, Ferris State University, University of Detroit, Mercy, Walsh College.	Six universities & one college	Three	Sponsors for the Michigan State conference include companies such as AT&T, Deloitt, Comcast, Symantec, Unisys, IBM, Cisco, MicroSoft, Motorola, ITC, Sprint, etc.	The State is pulling together a $3 billion private public initiative, "Pure Michigan Business Connect" to promote entrepreneurship to capital and a 'cyber security business environment'	Good

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
MN	The State through the collaboration with the non-profit organization, Advance IT Minnesota, is positioning Minnesota as a top-ten regional economy for information technology careers as measured by total IT-related employment. Through a strong quality education system which has increased enrollment in IT 76% since 2006.	Six: Inver Hills Community College and Minneapolis Community and Technical College are CAE/2Y. Capella University, Metropolitan State University, St Cloud State University and the University of Minnesota are all CAE/IAE.	Four universities & two colleges	Two	Companies: Honeywell, Alliant Tech Systems Inc., etc.	No data	Rather good, though can be even better.
MS	The State's cybersecurity profile and prominence is tied closely with the success and maturity of Mississippi State University (MSSU). The State has updated its cybercrime, cyber bullying and cyber stalking laws. The website is clearly laid out a policies are up-to-date. The state and MSSU has close ties to the FBI and DHS.	Mississippi State University is the only university ranked as a CAE in Mississippi; but the school holds all three designations, CAE, CAE-R and IA. The University has a strong reputation for digital forensics and working with veterans, collaborating with the FBI, DHS and other three letter agencies.	MSSU is ranked by the Ponemon Institute as the third best university to study cybersecurity in the country.	A fair number of military installations, Columbus and Kessler AFB, Camp Shelby Army Base and the Navy's Gulfport Battalion Center and the Naval Air Station (NAS) Meridian. Stennis Space Center	Companies: Apex Lockheed Martin, Raytheon, etc.	No data	Relatively good

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
MO	Missouri's Mission for cybersecurity is to promote and provide expertise in information security management for all state agencies and support national and local homeland information security efforts. Their Vision is to be a leader in preserving the confidentiality, integrity, and availability of state data and dependent resources while maintaining efficient and effective operations. Missouri passed cyber bullying and cyber stalking legislation in 2013.	Missouri has two centers of academic excellence, Missouri University of Science and Technology (CAE/IAE,CAE/R and the University of Missouri- Columbia, a CAE/IAE.	Seven universities	Two	Companies: Boeing, IBM, L3 Communications, Booz Allen Hamilton, Honeywell, MasterCard, etc.	No data	Relatively good
MT	Montana has a standard data breach notification laws (2-6-504. Notification of breach of security of data system & MONT CODE ANN § 30-14-1704: Montana Code - Section 30-14-1704: Computer security breach) that can be found at http://leg.mt.gov/bills/mca/2/6/2-6-504.htm. The state government provides a relatively exhaustive information security webpage (http://infosec.mt.gov/default.mcpx) and the state does have a CISO position as of 2013.	Montana is one of a just a handful of states that do not have any NSA approved centers of excellence.	One university & one college	Montana does not host any major cybersecurity research centers (national labs, FFRDCs, etc.) and the bulk of their research on IA is by academics.	Montana does not have a large specialized cybersecurity industry. There are a number of small boutique security and analytics companies that have taken advantage of Montana's low cost of living.	Using NSF funding University of Montana created a new Cyber Innovation Laboratory dubbed "Cyberlab" that is focused on IA and other relevant tech topics.	Rather low, though can be improving.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
NE	They have fairly strong data breach laws, a proactive state government. Their state government has a good reputation and hosts conferences and is active in outreach and organizing. Nebraska has a fairly standard and robust set of data breach notification laws with their Nebraska Revised Statute 87-801:807 that were first enacted in 2006. The state has a published IS policy updated as of 2013 that can be found at http://nitc.nebraska.gov/standards/8-101.html The state has a specific but limited cybersecurity web presence with http://www.cio.nebraska.gov/cyber-sec/index.html.	There are two NSA approved CAEs at the University of Nebraska at Omaha (UNO) and Bellevue University.	Two universities	Nebraska does not have the national labs or FFRDCs found in other states but their academic community appears to be relatively active and cooperative in cybersecurity studies.	Aside from the ubiquitous military industrial complex companies that work in cybersecurity and a number of smaller information security consultancies there are not many large specialized cybersecurity firms in Nebraska.	No data	Relatively good, but can be better.
NV	The state has some of the more stringent data breach and data security laws on its books. Particularly, Nevada has mandated PCI-DSS for companies operating in the state with payment cards. Nevada also has a CISO position with an Office of Information Security located in their Enterprise IT department. Since 1999 Nevada has had a Technological Crime Advisory Board that focuses to some degree on electronic crimes like identity theft, online fraud, etc.	Nevada has one NSA center of academic excellence with the University of Nevada Las Vegas.	Two universities & one college	Historically, Nevada has been very involved in nuclear testing and nuclear security and some of these agencies have limited cybersecurity R&D mission sets related to protecting the nuclear stockpile and weapon design information.	The enormous gaming industry has considerable interest in cybersecurity but specific information is not particularly easy to come by since the companies are highly competitive. The defense industry also maintains facilities in Nevada providing consulting and R&D services (CACI, Lockheed, etc.).	The historic relevance of nuclear energy and weapon testing means there is some cooperation between the state of Nevada and its companies/agencies and the US Department of Energy.	Can be better.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
NH	New Hampshire has a fairly robust data breach notification law that incorporates many of the elements found in other states throughout the US. NH has a devoted cybersecurity webpage on the state government's Information Technology site offering best practices, guidance, and basic threat alert information. The site can be viewed here: http://www.nh.gov/doit/cybersecurity/	New Hampshire has only Dartmouth College which holds the CAE-Research designation.	Two universities & one college.	There are no national laboratories or Federally Funded Research and Development Centers located in New Hampshire. That said, Dartmouth College developed and currently managed the Institute for Information Infrastructure Protection (I3P).	New Hampshire expects to see "professional, scientific, and technical services . . . [to grow] nearly 24 percent" between the years of 2010 and 2020.-- http://www.cybersecurityu.org/new-hampshire-steady-economy-attracts-cyber-professionals/ Some major information security employers in the state are BAE Systems, Bank of America, the State Government of NH, and Liberty Mutual.	Dartmouth College collects considerable grants (cursory search of awards is well over $2,000,000) from federal funding sources.	Rather good considering its relatively small size.
NJ	Data breach and cyber-bullying laws with a very involved state government and state police force. New Jersey has a number of cyber related government offices and bodies including a state ISAC, a department of information security with a portal, and a state homeland security & preparedness organization with a cyber-mission. The state police also have an information security unit and other IT related groups working on technology crime and researching means by which crime can more effectively be dealt with through leveraging technological assets. They also appear to have Cyber Aces and Cyber Patriot programs running that seek to educate and develop cyber talent.	Six CAEs with a variety of academic research centers contributing to theory and practice	Six universities	New Jersey has one FFRDC with the Princeton Plasma Physics Laboratory, to research cutting edge physics and nuclear fusion. Their cybersecurity relevance is nebulous at best. The major research and practice centers are located at the state's many educational institutions.	New Jersey is slotted as a major growth state for tech jobs and has established clusters in the financial services and bio-tech industries.	No data	Rather good, though can be even better.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
NM	The state is among the last in the US to enact any sort of comprehensive data breach protection law, going without such a statue until early 2014. NM has an ISAC as part of the compulsory national strategy and they have state-level homeland security and emergency management office. The state IT department publishes their security policies which appear fairly standard.	Two	Two universities	Sandia National Laboratory and Los Alamos National Laboratory: SCADA security, analytics, education, insider threat detection, energy grid security, quantum cryptography, malware classification, etc.).	New Mexico has a couple of industrial clusters with some relevance to cybersecurity. The presence of Kirtland AFB and a number of national labs bring in many Aerospace companies like Honeywell and Lockheed. There is some tech involvement (small Intel plant, etc.).	The University of New Mexico's Center for Information Assurance Research and Education has a SFS program.	Rather good, but can be better.
NY	New York is following close behind California in the legislative aspect of cyber regulations. Their focus is on financial and business repercussions of cyber security and the impact to national and international financial systems. In 2013 Governor Cuomo established a Cyber Security Advisory Board to guide state government on developments in cyber security and make recommendations for protecting the state's critical infrastructure and information systems. New York's governor is working to position New York as a leader in cybersecurity to attract the growing industry of cyber-related business to the state. Focus on the banking industry is a major strategy and NYS Department of Financial Services has "'required' 200 banks to assess cyber policies and processes."	Eight	Ten universities & two colleges	Three	There is an extensive list of accounting, consulting and law firms focused on the growing sector of cyber security related business.	No data	Very good

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
NC	As of October 1, 2009, entities doing business in North Carolina will be required to both provide more detailed data breach notices to individuals and be more forthcoming with the state's attorney general. NC DOJ provides best practice information to residents through alerts and news articles on their webpage. North Carolina has created a cyber-information sharing and analysis center that is part of the larger Multi-State ISAC. The NC-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure from state agencies and providing two-way sharing of information between and among the state agencies and with local government where permissible. NC has an office of Enterprise Security & Risk Management that provides state information security policies and procedures, awareness and training services, threat response, and secure IT procurement directives as part of the NC CIO's and CISO's responsibilities. The NC National Guard is being utilized for state cyber exercises	There are four NSA CAEs located in North Carolina at UNC-Charlotte, East Carolina University, NC State University, and North Carolina A&T State University.	Six universities & several colleges	There are research centers working on the majority of key cybersecurity topics with special attention being paid to big data, high performance computing, electric grid security, and embedded systems security.	The Research Triangle Park's security relevant tenants are as follows: IBM, Cisco, NetApp, Red Hat, EMC, GE, Lenovo, Qualcomm, Sony Ericsson, and Verizon and others. There are numerous bio-tech firms as well as a large DuPont chemical facility that likely contribute to some of the state's focus on protecting IP and securing data. NC is also home to Duke Energy which is absolutely one of the largest energy utilities in America and thus there's considerable focus on grid security, next-gen cyber physical systems, and embedded systems security. There is also huge interest and activity in big data and cloud computing. NC State is the alma mater of the founders of the software and analytics giant SAS and they maintain a large presence in the state.	The state's many collaborative research projects that span academia and industry attract fairly enormous funding from the NSF, DOD, and Intelligence Community. NC cyber research projects include a $60 million funding grant from the NSA and more than 20 currently active NSF cybersecurity grant awards that exceed $500,000.	Good

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
ND	North Dakota has a fairly standard data breach notification law on their books that was last updated in 2013 to include a person's health insurance information. They also have a cyber-bullying law in place as of 2013. The state government does have an office of IT Security and there is a state CISO. The ND state government's IT Security department maintains a webpage with best practices, alerts, and other guidance but it appears to be only infrequently updated. There exists a ND state government office focusing on homeland security and emergency services but there appears to be limited focus on cyber planning or exercises. The state is part of a Multi-State ISAC through DHS.	None.	One brick and mortar cybersecurity degree program at an institution called Rasmussen College in Fargo/Bismarck, ND. One place offering Forensics specialization at Southwestern Community College.	No evidence of private, public, or pseudo-public institutions or groups engaged in specialized cybersecurity research or practice.	Outside of the ubiquitous presence of Military Industrial Complex companies that do cybersecurity contracting there appears to be little commercial focus on cybersecurity in ND.	No data	Low.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
OH	Ohio has a fairly standard data breach notification law and they do have both a CISO and a Chief Privacy Officer for the state. The state does maintain a centralized privacy and security webpage to inform citizens about cybersecurity issues and to offer best practices guidelines for its residents. Past cybersecurity incidents (Anonymous hacking the state's web portal) seem to be pushing the state forward on cybersecurity.	Four (Air Force Institute of Technology, Ohio State University, Owens Community College and Sinclair Community College).	Ohio has four centers of excellence and a handful of other four year schools providing cybersecurity education. The state also has a large quantity of cybersecurity education being delivered through the two-year community college system. Altogether: eight universities & four colleges.	The state does have a number of large research universities like Ohio State and Cincinnati working on information security.	Companies: Verizon, Booz Allen Hamilton, JP Morgan Chase, Northrup Grumman, GE, IBM, Battelle	The Ohio Third Frontier Commission approved $5 million to support the Columbus Collaboratory, a multiple industry partnership to make Ohio a leader in advanced analytics and cybersecurity. A $20 million investment will come from American Electric Power, Battelle, Cardinal Health, Huntington Bank, L Brands, Nationwide and OhioHealth.	Good

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
OK	Oklahoma clearly defined its IT/Cybersecurity policies and procedures in 2003 with updates to their on-line manual in 2011. The state meetings regularly with its agencies and conducts quarterly meetings, table exercises and integrates their activities with the OK Homeland Security Department. The "Oklahoma Computer Crimes Act" initiated 1984 with updates related to cybercrimes, initially crimes involved with computers. http://www.forwardedge2.com/pdf/OK-laws.pdf; penalties ran from $5000 to $100,000 in penalties with jail time. 24 Okla. Stat. § 161 et seq. passed in 2008 lays out guidelines for security breech notification within Oklahoma. The state is running the Oklahoma's Cyber Command.	Oklahoma has six Centers for Academic Excellence and Research. Four are two year schools: Francis Tuttle Technology School, Oklahoma City Community College, Oklahoma Department of Career & Technology and Rose State College. Oklahoma State University and University of Tulsa are the four year CAEs.	Within the 29 technology centers at 58 campus sites, a range of cybersecurity courses, including networking through higher level certification courses at the CAE-R 2Y are available.	Three	Oklahoma has a strong DHS presence, with the major accounting firms, Deloitte, Price Waterhouse; Microsoft, major defense contractors and smaller home grown companies have positions relative to cybersecurity work at Fort Sills and Tinker AFB. The major companies, Microsoft, Google, CISCO and others have a presence in Oklahoma.	Oklahoma's 2004 NSF $3 million grant built a strong 2 year/4 year educational network. In 2007 an additional $2.7 million developed a deeper connection to workforce development.	Good

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
OR	Oregon has a standard data breach notification law on their books that was enacted in 2007 (§ 646A.604). Additionally they have the Oregon Identity Theft Protection Act (http://www.cbs.state.or.us/dfcs/id_theft.html) and proposing digital privacy legislation. The state government offers a fairly standard website for enterprise security and information security resources, providing basic guidance, best practices, and news related to information security. Oregon participated in the Department of Homeland Security's CyberStorm IV exercises. Through CS IV, DHS designed, conducted, and evaluated exercises for seven states including: Maine, Oregon, Washington, Idaho, Missouri, Mississippi, and Nevada. Oregon has taken efforts to extend information security learning down to elementary and high school level education. The Education Information Security Council (EISC) is responsible.	The only Center of Academic Excellence in Oregon was located at Portland State University (PSU). The National Security Agency (NSA) designated Portland State University as a Center of Academic Excellence in Information Assurance Education in 2003: http://www.pdx.edu/news/nsa-designates-portland-state-quotcenter-academic-excellence-information-assurance-educationquot But not anymore: https://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml	The educational component is relatively small but there appears to be active engagement and research going on at schools like Portland State, Univ. of Oregon, and Oregon State University as well as a number of options for two-year education.	The state does not have major cybersecurity relevant national labs or FFRDCs but has a number of organizations and institutions engaging in IA research both privately and publically. At University of Oregon there are a couple of ongoing research partnerships and academic centers performing cybersecurity research, publishing, and tool building.	The state has a respectable tech and software industry base making security products, solutions, and hardware. According to an OSU news article "there are about 20 companies in Oregon doing computer security-related work, one of the largest concentrations of cyber-security industry experts in the nation." -- http://oregonstate.edu/ua/ncs/archives/2002/aug/oregon-front-lines-fighting-cyber-terrorism Specifically, some of those companies includes Flir Systems, ID Experts, EID Passport, Kryptiq and Tripwire. As well as, Mentor Graphics and Intel – working with its McAfee subsidiary – are developing hardware-based technologies to guard against online snooping. As part of their outreach program on cyber education, Oregon has set up "The Oregon Centre for Cyber Excellence (OCE)". The purpose is to be a national asset to advance substantially the knowledge and educational strategies for cyber-education. They are collaborating with Colleges and Universities in the state.	Source of Funding: Federal support, industry funding and National Security Foundation (NSF), Intel, Google, MIT Lincoln Labs, Battelle and ARO. Total research funding to date is about $8.49 million.	Relatively good.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
PA	PA's Governor has spoken about the importance of public/private partnerships in securing critical infrastructure. Pennsylvania's Information Security Office has a pretty comprehensive website with information for residents about their department, security awareness, and resources. The Pennsylvania Information Sharing and Analysis Center (PA-ISAC) was established to address the Commonwealth of Pennsylvania's cyber security readiness and critical infrastructure coordination. This initiative is led by the Chief Information Security Officer for the Commonwealth of Pennsylvania's Office for Technology, responsible for leading and coordinating the Commonwealth's efforts regarding cyber readiness and resilience. Pennsylvania has a CERT team: PA-CSIRT, the Commonwealth of Pennsylvania's Computer Incident Response Team.	Pennsylvania currently has 7 NSA/DHS-designated academic Centers of Excellence, four of which offer SFS scholarships. Carnegie Mellon University (CMU) is a national leader in cybersecurity research and education and one of the few NSA-designated CAEs in Cyber Operations.	Three out of seven PA schools were ranked in the top 10 for cybersecurity education by the Ponemon Institute (Carnegie Mellon, U of Pittsburgh, West Chester U).	PA has seven of the nation's leading cybersecurity research centers, most notably at CMU.	Companies: The National Cyber-Forensics & Training Alliance, H-Bar Cyber Solutions, Wombat Security, Dell, Software Engineering Institute at Carnegie Mellon University, Lockheed Martin, BAE Systems	NSF Scholarship for Service grants awarded to four universities.	Very good.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
RI	In 2011 the Rhode Island Cyber Disruption Team (RICDT) was established, whose mission is to prevent and respond to cyber security events and defend the security of critical infrastructure. The RICDT is comprised of members from the Rhode Island State Police Computer Crimes Unit and individuals representing higher education, hospitals, finance, utilities and defense. The following year the state released RI Statewide Cyber Strategic Plan. RI is one of a few states—including Massachusetts, California, Connecticut, Oregon, Maryland, and Nevada—have also enacted laws requiring businesses to maintain data security standards to protect state residents' personal information from being compromised.	University of Rhode Island is the only CAE CAER/ IAE in the state.	Three universities	Two	Companies: Cybercoders, The Judge Group, Corvus Technology Resources, CVS, Atrion, CVS Caremark, CharterCARE Health Partners, OSHEAN, Corvus, Technology Resources, Carousel Industries, GTECH	Verizon Foundation has awarded a $15,000 grant to the Salve University to further the Pell Center for International Relations and Public Policy's efforts in helping to bolster cybersecurity in Rhode Island companies.	Rather low, can be better.
SC	South Carolina instituted cybersecurity stalking, harassment and anti-bullying laws in 2012-13 legislative sessions. The State has awarded Deloitte contracts for incident response. The initial reports – SC needs to establish and mature its cybersecurity profile across the state government and there will be a need for long-term commitment of funding to bring the state up to an acceptable level of performance. As this report was filed in 2014, legislation is in the process of being developed. The State connects to MSISAC and DHS.	University of South Carolina is the only CAE/IAE - is a new center with a focus on engineering – specifically securing wired and unwired network and security protocol development for networks and distributed systems.	One	One	The Advanced Security Technology Research Alliance (ASTRA).	ASTRA has received a $50,000 grant from the Trident Workforce Investment Board to offer two training programs in the Charleston area.	Low, needs improvement.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
SD	The state is one of three in the US that has failed to set up data breach notification laws and appears to engage very little in state government cybersecurity promotion, awareness, and education. Their cyber security legislation is pending for 2015. There is a very limited cybersecurity web portal provided by the state government that largely offers links to federal resources on information assurance.	Dakota State University is the only CAE/IAE in the state South Dakota and received the designation in 2012-13.	The state has a small education system but is home to a premier cybersecurity school with Dakota State University. Its B.S. in Cyber Operations is being augmented with a new doctoral degree in cybersecurity in Fall 2014. South Dakota State University (SDSU) also offers degree programs in information security.	There are no major research centers or companies but two interesting academic research project.	Secure Banking Solutions (SBS). The need for security professionals is also for companies: SCN Communications, S2Technologies, Stinger Ghaffarian Technologies, Black Hills Corporation.	In 2013 the Legislature appropriated $900,000 to fund Dakota State University's information systems programs and cyber security programs.	Rather low

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
TN	Tennessee State Government seems to have a limited presence on cybersecurity. The Governor has proclaimed October Cybersecurity Month and the Department of Finance is taking the 'lead' with a 38 page Policy Manual. Tennessee has enacted Cybersecurity Breach Law.	There are one two-year, Jackson State Community College, and three CAE/IAE universities: Fountainhead College of Technology, University of Memphis, and University of Tennessee at Chattanooga.	Four universities and one college	Oakridge National Laboratory (ORNL)'s Cyber Information Security Research (CISR).	There is extensive corporate presence buzzing around ORNL and the rest of the state. Deloitte, Addeco, Apex Systems, Cadre Information Security, Booz Allen Hamilton, IBM, The Hinkle Group have a presence in the state.	No data	Relatively good
TX	This state is VERY invested in cybersecurity. State cyber laws and policies are outline in the "Texas Cybersecurity Framework" http://www.dir.state.tx.us/security/policy/Pages/framework.aspx	Texas has 16 NSA/DHS-designated Centers of Excellence.	Dozens of colleges/universities. UT San Antonio was ranked as the #1 university for cybersecurity by HP / Ponemon in 2014.	San Antonio has been dubbed "Cyber City USA" due it being the home of the Air Force Cyber Command as well as the National Security Agency's Texas Cryptology Center, a new National Security Agency data center.	Nearly 80 defense contractors, including dozens focused on information security.	Four of the CAEs offer SFS scholarships. Also, NSF grant award of $284,000 to The San Antonio College (SAC) Department of Computer Information Systems (CIS)	Excellent

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
UT	"We have a rich history in defense, IT, and in a lot of other business sectors, as well," said Gary Harter, Executive Director of Veteran's Affairs with the Utah Governor's Office of Economic Development." A number of companies tell us they like coming to Utah, and they like hiring in Utah, because they find good success with employees in Utah who can readily get security clearances." The state also offers a number of incentives for business, including low energy and utility costs and reasonable permitting and regulation.	Only has one university that is designated as a CAE.	Four universities.	NSA recently built their massive data center there. Also, Space Dynamics Laboratory – Utah State University.	Salt Lake City was named by ClearanceJobs.com as one of the top 5 cities for cybersecurity companies. There is a notable presence of government and contractors in the area. Companies: Raytheon, FireEye, AccessData, Northrop Grumman	Utah Valley University received a $3 million grant for cybersecurity training from the Department of Labor.	Relatively good.
VT	The governor has integrated services and policies reflecting a well-integrated approach to communicating with multiple audiences through an easy to use state website: www.itsecurity.vermont.gov. IT policies ranging from 2004 to 2012 have been updated to reflect Vermont's review of 'hot topics' such as Mobile Devices. Cyberbullying is covered by State Law 16 and passed a Security Breach Notification Law in 2012.	Vermont has two centers of academic excellence: Champlain College and Norwich University.	One university and one college.	Four	S2Technologies There were 21 open cybersecurity positions through Indeed related to activities at St. Albans AFB in Vermont.	Pwnie Express in 2013 raised $5.1 million to test wireless devices and networks in remote locations.	Relatively low.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
VA	Virginia has two distinct security breach disclosure and notification laws that separately cover both personal information and private healthcare related information. The laws are similar to those found in many US states and provide definitions on the types of data to be secured and the mechanisms by which companies must notify victims of a breach. In 2014, Virginia governor Terry McAuliffe created the Virginia Cybersecurity Commission that has been tasked with identifying high risk security threats, promoting cybersecurity awareness and offering expert input related to the security of state networks and information assets. The Commission includes former US Cybersecurity "Czar" Richard A. Clarke.	The state is home to seven NSA Centers of Academic Excellence and those programs benefit greatly from their relative proximity to the US federal government.	Eight universities and one college.	Virginia is home to a huge number of federal agencies that have cybersecurity responsibilities. DHS has NCCIC and US CERT in Arlington. Additionally, MITRE Corp has long maintained a large facility in Northern Virginia.	General Dynamics, Lockheed Martin, Boeing, Booz Allen	Massive funding…given proximity to DoD, NSF, NASA, etc.	Good

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
WA	Washington State enacted an anti-cyber-stalking group early on. The legislature has enacted cyberbullying legislation and there is pending legislation in HB 1365-2013-14 requiring cities and counties to provide higher levels of security for their courts. Washington State is active in the MRSC and has a strong relationship with the Department of Homeland Security (via PRISEM). Association of Washington Cities promotes cyber security across the state.	One university and two colleges.	Six universities and seven colleges.	Pacific Northwest National Labs headquartered in Richland, WA, PNNL maintains offices in Seattle and concentrates cybersecurity research in several areas.	Seattle and the East Side, Bellevue, Kirkland, Redmond support strong cyber security business climates. Washington State is the home of Microsoft, Amazon, Starbucks, Boeing; companies with high cyber security needs. Google has developed a presence and IBM, Booz Hamilton, Deloitte and a myriad of government focused contractors are attracted to JBLM, Fairchild AFB, Bangor Naval Base/Bremerton Shipyard. Additional companies include Verizon Wireless, T-Mobile, etc.	PRISEM, in collaboration with WA State Dept. of Commerce, has received funding to transition to a non-profit business model.	Relatively good, but can be even better.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
WV	West Virginia's Office of Technology Cyber Security Program won an award in 2011 for Risk Management Initiatives. Executive Order 6-06 called for the formation of an Executive Branch Information Security Team and a Privacy Management Team. The Governor's Executive Information Security Team (GEIST) was subsequently established which enlisted high-level departmental operatives to extend the reach of the Office of Information Security and Controls. An Information Security Strategic Plan was developed and, over time, resources and tools have been acquired to focus on the information and cybersecurity challenge of overall risk reduction through strong controls and heightened awareness. In addition, an audit function was established at the Office of Technology.	Two	One university and one college.	Two	Companies: Lockheed Martin, TASC, SecureStrux LLC, FireEye, Mitre Corporation, Criterion Systems	None found.	Relatively low.
WI	The state has a "Ready Wisconsin" site, part of WI's emergency management efforts and in line with DHS's "Ready" campaign, promotes cybersecurity awareness and safety tips and links for citizens. There is also a state Bureau of Security.	None	One university and one college.	Three	Companies: Wisconsin Security Research Consortium, USIS	Researchers at UW-Madison received a portion of a large federal grant for developing secure software for infrastructure systems. Also, Collaborative Research grant from the NSF for Wisconsin Collaborating Campuses on Cyber Security.	Low

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
WY	Governor Mead has been pushing for betting Internet access in the state of Wyoming. The governor is aware of cybersecurity issues and the state government website provides helpful links for information/awareness. WY has pretty standard Electronic Crime statues.	None	One college.	One	Companies: Green House Data	None found.	Low.

State	State involvement / Legal field	CAEs	Cyber security degree programs	CS research centers / facilities	Industry	Grants	Overall
PR	According to the IC3 Internet Crime Report for 2013, Puerto Rico ranked ninth globally in terms of total victim complaints related to cybercrime with 550, placing the island above such nations as Brazil, France, Germany, Russia, Italy, China and Japan. A large proportion of these attacks are targeted at banks with the intent to steal sensitive data, including account numbers and other financial information. In Puerto Rico, there are two units dedicated to investigating cybercrimes on the island: the Cybercrimes Division at the Police Department and the Cybercrimes Investigation Unit at the Justice Department. Several attempts were made to establish a definitive public policy on the prosecution of cybercrime through local House Bill 2408. The bill aimed to create a "Cyber Code," but was ultimately defeated on the House floor in April 2010. The House Resolution 545, which calls for an investigation into the need for the Police cybercrime division to receive additional funding, is currently under review by the House's Internal Affairs Committee: http://www.caribbeanbusinesspr.com/prnt_ed/puerto-rico-among-the-top-10-cyberattack-targets-globally-10680.html	One - Polytechnic University of Puerto Rico http://www.pupr.edu/information-assurance-and-security/	One university.	None.	Microsoft, Cisco, Oracle, Hewlett-Packard have operations in Puerto Rico. Infotech Aerospace Services (IAS), Honeywell Aerospace, Lockheed Martin, Pratt & Whitney and Hamilton Sunstrand are also present: http://www.pridco.com/industries/Pages/Information-Technology.aspx	In 2014 the NSF's grant No. DUE-1438838 funded the University of Puerto Rico-Rio Piedras with $299,982 to advance cybersecurity knowledge in Puerto Rico. "This project, at the University of Puerto Rico-Rio Piedras, is the first step in creating a research, development, and education program in cybersecurity at the institution." http://ccom.uprrp.edu/~atackpr/index.php?mact=News,cntnt01,detail,0&cntnt01articleid=4&cntnt01returnid=15	Relatively low.

CONCLUSIONS

Based on the resultant table we can divide all the states, depending on their level of cybersecurity development, into six categories, from "Excellent" to "Low".

The first category, "Excellent", consists of two exceptional states: Maryland and Texas. Each of them has 16 CAEs, tens of universities and colleges offering cybersecurity programs of various levels, very serious cybersecurity facilities and research centers, dozens of powerful cybersecurity companies and government contractors.

The second category, "Very good", consists of four powerful states: California, Illinois, New York, and Pennsylvania. Each of them has seven or eight CAEs, prominent educational cybersecurity programs at university and college levels, leading cybersecurity research centers, many cybersecurity companies and governmental contractors, and a lot of funds granted to the local cybersecurity-related institutions.

The third category, "Good", consists of 11 states in which the level of cybersecurity development is good and can be considered as adequate taking into account these states' other parameters: Alabama, Colorado, DC, Florida, Massachusetts, Michigan, New Jersey, North Carolina, Ohio, Oklahoma, Virginia. Each of them has from four to seven CAEs, sufficient numbers of the academic programs in cybersecurity, related research centers, government contractors and cybersecurity-related companies.

The fourth, most populated, category is "Rather good". These 16 states have relatively good level of cybersecurity development, but, taking into account their potential, can do even better: Arizona, Connecticut, Georgia, Indiana, Kansas, Louisiana, Minnesota, Mississippi, Missouri, Nebraska, New Hampshire, New Mexico, Oregon, Tennessee, Utah and Washington. For example, some of them definitely can have more CAEs than they have currently: Arizona (3), New Mexico (2), Oregon (0), Utah (1), Washington (3).

The fifth category consists of 12 states where the level of cybersecurity development is relatively low, but they, at least, conduct visible efforts to improve the situation: Delaware, Hawaii, Idaho, Iowa, Maine, Montana, Nevada, Rhode Island, South Dakota, Vermont, West Virginia, Puerto Rico. If they will continue this positive trend, then can hope to move to the higher level of cybersecurity development rather soon.

Finally, the last category is "Low". It consists of seven states with the lowest level of cybersecurity development, and it looks that they are not making enough efforts to improve the situation: Alaska, Arkansas, Kentucky, North Dakota, South Carolina, Wisconsin and Wyoming. For example, altogether these seven states have only four CAEs, while four of them don't have CAEs at all.

Overall, we can come to the conclusion that, under the current difficult global cybersecurity situation, when powerful adversarial to the USA nations rapidly develop their cybersecurity potential, majority of the American united states underperform in the cybersecurity area. Specifically, we need more and better prepared human resources to be ready to withstand those global threats. More cybersecurity educational programs with courses specifically targeting those global menaces should be developed and funded in our country. Only in such a way we will prepare adequate number of cyber warriors familiar enough with our potential global enemies and their cybersecurity capabilities, tactics and strategies.

BIBLIOGRAPHY

[1] Arati Prabhakar, DirectorDefense Advanced Projects Research Agency, Defense One Conference, November 2014

[2] Keith B. Alexander, The Next Wave Introduction, NSA/CSS website, 2012, https://www.nsa.gov/research/tnw/tnw194/article2.shtml

[3] James Clapper, Intel Heads Now Fear Cyber Attack More Than Terror, Quote to Congressional Testimony, March 2013

200+ DHS/NSA Centers of Academic Excellence exist across the United States at various colleges and universities, mostly concentrated around the Beltway, the East Coast seaboard through Texas. While these have been engines of dissemination for emerging government standards for cybersecurity education and workforce development (NIST/NICE initiative), there are thousands of universities and colleges that are not aboard and are graduating students with an unawareness of cybersecurity.

[4] Tripwire, Cyber Security Tops Intelligence Community's 2014 Threat Assessment, Feb 10, 2014

[5] InfoSec Institute, Cyber Threat Analysis, http://resources.infosecinstitute.com/cyber-threat-analysis/

[6] David Bisson, NSA Chief Concerned about Cyber Attacks on U.S. Critical Infrastructure, Wired Magazine, 21 November 2014.

[7] John A. Van Messel, Unrestricted Warfare: A Chinese doctrine for future warfare. Marine Corps University, June 2005

[8] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao; The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure; Project 2049 Institute; November 11, 2011

[9] "Cyber Security Dictionary". 2 Jan 2012. Retrieved 23 March 2014.

[10] Walt Boys, "Back to Basics: SCADA", Automation TV: Control Global - Control Design, 18 August 2009.

[11] Anshul Thakur, SCADA, Engineering Garage, http://www.engineersgarage.com/articles/scada-systems.

[12] Eric Byres, SCADA security Basics: SCADA VS ICS terminology, Tofino Security, 5 September 2012 (https://www.tofinosecurity.com/blog/scada-security-basics-scada-vs-ics-terminology)

[13] Anshul Thakur, SCADA, Engineering Garage, http://www.engineersgarage.com/articles/scada-systems

[14] Arati Prabhakar, Director, Defense Advanced Projects Research Agency, Defense One Conference, November 2014

[15] United States Government Accountability Office. Cyber Security, National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO. February 2013

[16] Martin C. Libicki, David Senty, Julia Pollack. Hackers Wanted, An Examination of the Cyber Security Labor Market, RAND. June 18, 2014
[17a] probability of 1

[17] US Cyber Command, Cyber Mission Force Operation Plan (unclassified briefing)

[18] United States Government Accountability Office. Cyber Security, National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. GAO. February 2013

[19] Martin C. Libicki, David Senty, Julia Pollack. Hackers Wanted, An Examination of the Cyber Security Labor Market, RAND. June 18, 2014.