Project Narrative

Intellectual Merit

Each day companies and organizations are becoming more and more reliant on technology to store and send information, especially the internet. This creates an equally increasing vulnerability to cyber-attacks for these companies and organizations as well as an increasing obligation to protect information. There is a need for knowledge in cyber security in every career field and discipline. The modern workforce must have this knowledge and the skills to handle the cyber threats. Without a properly trained workforce, the world will continue to fall victim to cyber-criminal activity, which will have severe consequences and catastrophic results. If an cyber attack is done just right a criminal can cripple and entire system and an entire company.

c-Watch - Advance the knowledge of Students

c-Watch is a three-track online education program that teaches students how to identify and report on potential cyber threats and builds skills in cyber security necessary to do so. The three tracks c-Watch consists of are threat hunters, social media, and geopolitics. The first two tracks in the c-Watch program, threat hunters and social media, perform the investigative work within the program. In other words, these tracks focus on finding and identifying potential threats. The main difference between these tracks is the type of data they are looking at and where it is coming from.

Threat hunters actively monitor information and traffic that travels across networks that are used at sporting events or within sports organizations. These threat hunters will look for common forms of cyber attacks including malware, intrusions, DDos attacks, and phishing scams. Attacks can occur at any point in time for unknown reason. The purpose of this track is just to identify and prevent attacks, then be able to report on them.

The second track in c-Watch, the social media team, looks at various aspects of social media including trends, specific traffic during certain times, and bots sending out fake information. Trends and spikes on social media usually mean something is occurring in the real world or that something being pushed out as a disinformation campaign by bots. Bots will create accounts over and over and use these accounts to post trending hashtags repeatedly as well as to post stories. After that, these stories and trends will get picked up and re-posted by real accounts and overtime people will begin to recognize it as real information.

The last track in the c-Watch program, geopolitics, focuses on analyzing potential threats. With the geopolitics track we can gain an understanding on the motives and intentions behind cyber attacks. Once threats or potential problems are identified, they are handed to the threat analysis group in the geopolitics track. These analysts will then determine what threats are occurring and why by looking at the bigger picture internationally; they link the cyber-attacks to international

events. Analysts will also determine where the attack came from, who the hackers involved in the attack were, and who the target of the attack was. After gathering this information, the analysts build cyber-attack characterizations and profiles. These characterizations and profiles can be used to find patterns in what may seem to be completely unrelated cyber-attacks. Oftentimes criminals will use the same language or methodology in totally unrelated attacks. If that information is shared with other organizations, it will give them the ability to recognize these threat patterns which they can use to prevent attacks before they happen. After completing the c-Watch training students can then enter into the CrowdWatch program to gain further experience into cyber security.

CrowdWatch - Advance the knowledge in the field of Cyber Security

CrowdWatch is a program that uses crowdsourcing through c-Watch to acquire personnel from around the world to create a network of threat hunters to find and identify cyber threats. As mentioned before, the main goal of c-Watch is to acquire more trained professionals, certify them, and put them in an environment where they can recognize real time threats. In other words, the more skilled people that the CRI acquires in the c-Watch program, the stronger of a defense network there will be for finding, analyzing and preventing threats with the CrowdWatch program.

The CrowdWatch program launches pop-up Security Operation Centers (SOC) at major sporting events across the world. These operation centers will have the threat hunters and the social media team actively monitoring, to ensure the sporting event will go smoothly. These groups specifically monitor key components that are vital to the operation of the sporting event and components that could cause danger to people if targeted such as critical infrastructure. It is through these major sporting events sports organizations can obtain vital data that can be analyzed to find patterns in cyber-attacks and strengthen our understanding of methods used during these attacks.

Outline the general plan of work

The C-watch program goes up to twelve weeks and consists of a capstone at the end. One of the ways the CRI is attempting to do this is encouraging the creation of c-Watch clubs in universities. The CRI is currently partnering with universities to make the c-Watch program accessible to university students, so they can take advantage of the program. The CRI plans to create CrowdWatch clubs and expand them across multiple universities and to other entities involved in these programs. After students finish c-Watch, students will be trained and given hands on experience with cyber threats in the CrowdWatch program. Individuals in this program will research cyber threats, collaborate with each other, and participate in activities that help to build skills and expand their social network. This will help students to acquire both a

certification and valuable skills which gives them an advantage in the workforce regardless whatever of the career field they have chosen. The CRI does their capstones at major sporting events, in which they The CRI runs pop-up Security Operation Centers at major sporting events both nationally and internationally, which is also the capstones for the c-Watch program.

Four Factors of Success

There are four factors that would prove and determine that the CRI has achieved its goals. The first factor that would indicate that the CRI has achieved these goals is that it has successfully laid the groundwork and created the infrastructure for the c-Watch program to drive and support itself. The CRI does not intend to be a training organization through the c-Watch program. Instead, the CRI intends to develop c-Watch training outside of their organization and expand out to the CrowdWatch program. This will be mainly accomplished through the development of ClubWatch.

Another factor that would determine success is that the CRI has successfully established an incentivized market for cyber resilience and security. The CRI is trying to incentivize companies to take a proactive stance on cyber security by sharing info on cyber-attacks/threats with other organizations, mitigate these threats before they happen, and stay ahead of criminals by developing software and technology to defeat cyberattacks and so criminals can't break into systems. The dark web and black market have established an environment where anyone can perform crime for profit. Which is why establishing a proactive mindset with cyber security is essential. This goal seeks to basically incentivize cyber security and establish cyber resilience; creating a similar environment to that of cyber criminals in the sense that organizations are more motivated and encouraged to work together and proactively deal with cyber threats.

The third factor in success will be that the c-Watch program has cultivated a skilled workforce that is more knowledgeable and adept in handling cyber threats. Giving the current and future workforce the knowledge and skills to deal with cyber security not only benefits themselves, but the organization, field of study, and community in which they work in. This workforce would also be a valuable asset for the CrowdWatch Program. Our modern world is an online one; regardless of whatever field the individuals may peruse, this program will give them keen awareness of the dangers in the digital world and valuable knowledge and skills to deal with them. This program would help them to know how to develop more cyber resilient infrastructure within their workplace and allow them to be an advocate for a more proactive stance in the workplace towards preventing cyber-attacks.

The fourth factor in success will be that the CrowdWatch program has created a stronger defense against cyber threats. Handling real time data and active threats, the CrowdWatch program will

build a constantly growing repository of knowledge on cyber threats that can be shared with other organizations. Each of these factors play a vital role in the success of the CRI's objectives; however, success would be meaningless if there was no benefit for having the programs. This data can be shared with other organizations.

What benefits would accrue if the project is successful

If the c-Watch program is successful, then students will be given hands on experience with cyber threats and build valuable skills in the field of cyber security. The skills and certification these individuals acquire will give them an advantage in the workforce and will help to build a workforce that is more knowledgeable and capable with dealing with cyber threats. With a workforce that has a better understanding of cyber security, naturally this will also build a stronger defense against cyber threats and build a more cyber resilient community.

As mentioned before, if the CrowdWatch program is successful, the sports community will have a stronger defense against network for finding, analyzing and preventing cyber threats. If that information is shared with other organizations, it can be used to help protect those organizations from falling victim to the same type of vulnerability or attack. Another benefit of the success of the CrowdWatch program is that the CRI will have taken another major step in building a proactive community and incentivized market in cyber security.

Scalability

The CRI plans on increasing the adoption of both the c-Watch and CrowdWatch programs through partnering with universities to create clubs on college campuses, called ClubWatch. ClubWatch brings the presence of the CrowdWatch program to universities which in turn brings universities to the CrowdWatch program. This means that ClubWatch will not only increase the members of the CrowdWatch program, but also build a stronger and sustainable community. The c-Watch training program is intended for anyone in the community who has an interest in cyber security. The university outreach only helps to expand the reach of the programs and provide students with an additional resource.

Steps to broaden access and community adoption

For CRI, a huge part of broadening access and community adoption is done through university outreach with ClubWatch. ClubWatch makes both the c-Watch and CrowdWatch programs more accessible and affordable for students. Not to mention, ClubWatch also helps students to build the skills and a network of peers even prior to completion of the c-Watch training program and entrance into CrowdWatch.

Challenges addressed in training, education, and workforce development;

One of the main struggles college grads face is that that entry level jobs require experience. Yet, the only way to get experience is through a job. The experience these programs provide and the skills they build helps to change that for those going into Cyber Security. For example, during major sporting events, ClubWatch will contribute to defend against and analyze threats that target the event.

Advances in integrating skills into curriculum/instructional material

With just the c-Watch program alone, students gain access to activities and training in cyber security. However, by working directly in the field through CrowdWatch, members gain hands on experience with the latest threats and data on cyber-attacks. All of this training and experience is focused into a specialized track. c-Watch and CrowdWatch relate to cyber infrastructure in that they protect personal information and data from criminals. These criminals enter personal accounts in order to steal information such as security numbers, passwords, identify and sell it to black markets and/or dark web for profit. Additionally, c-Watch and CrowdWatch advance data science because they develop and improve software and technology to defeat cyberattacks. Another advancement these programs bring is advancements to engineering by designing the community resilience business model.

Broader Impacts Narrative

Discussion of the Broader Impacts of the proposed activities

One of the most difficult challenges we face today is the theft of data. Cyber thieves are able to sell information anywhere around the world. This has made online criminal activity significantly more profitable, giving cyber thieves an increasing incentive to break into systems and steal information. These cyber threats affect organizations, governments, and industries all over the world. Even the sports industry is vulnerable and affected by these threats. Sports events like the World Cup and Olympics have especially been a target for cyber criminals due to high visibility in the public eye from large amounts of attention caused by the news and other forms of media. In order to create a safer and more secure society, the Cyber Resilience Institute seeks to combat these threats through the c-Watch and CrowdWatch programs. On the Article IV from "Cyber Resilience Institute: Articles of Incorporation" mentions that "The business and purpose of the corporation shall be to help mobilize society to improve community cyber security and resilience through educational and scientific effort" (page 1). There are many implications of the c-Watch and CrowdWatch programs that will have a broader impact on society outside the realm of education. The first major impact of these programs is that they will help to protect personal information from cyber attackers. Members of the c-Watch program will learn how to spot a cyberattack on computer systems and sports networks. The second impact, these programs will have is the protection of critical infrastructure. In the past, there has been terrorism during sporting events and if this critical infrastructure is targeted, it can endanger the lives of those who attend these events. The hands-on experience members acquire through these events is priceless. Lastly, these programs will impact society by developing a stronger force of individuals who are willing to mitigate cyber crime and cyber terrorism.

Full Participation in (STEM)

CRI does have full participation for women, people with disabilities and underrepresented groups. In fact, CRI has no age limits on who take these two programs. Helen Robinson from *Business Journal*: "Training Cybersecurity experts through soccer, c-watch is ready for kick-off" interviewed Doug DePeppe about c-watch, and he states, "c-Watch trains students from wide range of age groups and educational background" (Robinson). The full participation of these two programs is that anyone and students at any age who is interested in cyber security can go into c-Watch and CrowdWatch if they can afford it. However, universities and the CRI itself are both making efforts to provide discounts for students. For example, University of Colorado Colorado Springs (UCCS) is currently developing a CrowdWatch club called ClubWatch. If an individual does not have the money to afford to go into these programs, the ClubWatch program will offer discounts and scholarships for c-Watch training depending on the individuals participation in the program. The Bachelors of Innovation degree program at UCCS is also looking into providing

scholarships for students looking into taking the c-Watch training. CRI has also provided discounts to universities for students.

Improved STEM education and educator development

CRI's c-Watch and CrowdWatch programs are both in the field of computer security as they help to educate in and defend against cyber threats. Both programs will help students to understand the causes of cyber threats in sports events and show the dangers of cybercrime. According to "c-Watch Training and the CrowdWatch Cadré," "Students and a university coordinator participate in a crowd-sourced environment over a period of several months that involves cyber threat platform training, trade-craft lectures, hunting and analyst tools, public policy scenarios, and an event-based experiential learning capstone. The license is with universities and provides students a cyber threat intelligence and information sharing virtual laboratory and curriculum, whereby participating universities create a course credit offering tied to the crowd-sourced environment or their students can register and transfer credit from a participating, license-holding university that offers course credit. Further, universities may develop additional derivative courses in the emerging spaces of cyber intelligence, information sharing and public policy" (*Cyber Resilience Institute*). Students will learn about cyber intelligence tradecraft, information framework sharing frameworks. They will experiment training on social media tracking and security operations. Students at any age will learn about cyber intelligence tradecraft, sharing frameworks, social media tracking and security operations. In conclusion, CRI plans to improve STEM education and educator development at any level.

Increase partnerships between academia, industry and others

CRI increase partnerships between academia, industry and others. CRI is currently partnered with U.S. Department of Homeland Security's National Protection and Programs Directorate (NPPD) within the Office of Cybersecurity and Communications. The U.S. Department of Homeland Security has helped CRI with…..Another partnership is universities. CRI partnered with universities such as University of Colorado Springs Colorado, Case Western Reserve University, Bellevue University, and Bowi State University, all who are already engaged in these programs. Right now, CRI has one hundred students participating in two Olympics games and collaborated with more than thirty universities' students involved in CRI (Stiles and Lippert). CRI is willing to expand their programs to university clubs to develop communities on campuses as well (DePeppe); for example, they want to have c-Watch and CrowdWatch accessible for every university student to have the opportunity to learn about cyber security. The CRI also wants to make it available to all individuals in general who may be interested in learning about cyber security.

Improve national security

For many years, cyber terrorism has been a problem in the United States. In the article "Cyber Security Protection Personal Data Online: First Report of Session 2016-17" points out that "Cyber-Crime is a significant and growing problem and affects all sectors with an on-line platform or service" (3). Cyber criminals are being paid to steal personal information, salaries, social security numbers and sell it to countries and/or organizations illegally. For example, if a hacker easily guessed a football player's login password and accesses the football player's personal account to get information, then the hacker can take the personal information and sell it to the dark web or sell it to a black market for profit. In order to improve national security, the c-Watch and CrowdWatch works to secure information and protect it from cyber attackers. As previously mentioned c-Watch and Crowdwatch train students how to protect information. Doug DePeppe and he explains that "c-Watch gives students access to practicing professionals in the field of threat intelligence and real-world experience in a SOC" (Robinson). The training, education and research workforce challenges students to collect and share cyber threats data.

Increase economic competitiveness of the US

CRI's increase economic competitiveness of the US is having C-Market by hacking in a good way. In Jason Lippert's article "Why CyberSecurity so Important?" states that cybercrime is $4 trillion dollars, and United States citizens are victims of Ransomware because families are introduced to hackers. Interestingly, more than 100 United States citizens are willing to pay more than 34 percent of people globally (Lippert). C-Market program is trying to balance the good way of hacking, and it would increase economic competitiveness by creating cyber security job opportunities, which C-Market will hire cyber security experts to work on web activities in order to protect information. CRI's C-Market is a market that helps citizen have their information protected from cyber criminals.

Enhanced infrastructure for research and education

Cyber Resilience Institute (CRI) has many different ways to enhance infrastructure for research and education. The first way the CRI does this is through the c-Watch program. The c-Watch program enhances infrastructure for education by giving students training and experience in Cyber Security they would not be able to receive outside of a job. c-Watch also provides students with activities that grant them access to real data. Another way is the CrowdWatch program enhances infrastructure in research through threat identification and analysis. By utilizing data collected from threat analysis, the CRI is able to enhance infrastructure for research by developing new tools, methodologies, and technologies to find threats and defend against them.

Stakeholders engaged and partnerships forged for collective impact

Cyber Resilience Institute (CRI) has many stakeholders engaged and partnerships forged for collective impact. The first one, CRI partnered with Information Sharing and Analysis Organizations (ISAO). ISAO "gather, analyze and disseminate information for protecting

computing assets from common threats" (Lippert). ISAO are groups that work with existing information sharing organizations, owners and operators of critical infrastructure, relevant agencies, and other public and private sector stakeholders (*ISAO Standards Organization*). ISAO is helping CRI to make cyber security more sustainable for the United States. Another one, CRI partnered with Cooperative Research and Development Agreement (CRADA). CRADA is helping CRI with find cyber threats quicker before the start of a sporting event. The last one, CRI partnered with Cyber Information and Collaboration Program (CISP). The CISP is a program that shares cyber threat information and collaborates with communities. In their defense of Homeland Security, they want to build a community of trust between with the Federal Government and entities across from different critical infrastructure sectors. They plan to leverage these relationships to increase information sharing and collaboration in order to improve network defense for the entire community (*Cyber Resilience Institute*). Both of them are information sharing and collaboration with DHS's critical infrastructure partners. CRI has worked with The Critical Infrastructure Key Resources Cyber Information (CIKR) and CIKR is currently helping CRI with building a community of trust. Overall, these are the stakeholders and partnerships of CRI.

New modes of discovery and use of advanced CI in research enabled

The Cyber Resilience Institute (CRI) researches threat identification and analysis. The first research is experience. Doug DePeppe had many experiences working with cyber security. Doug helps "businesses design and implement commercially reasonable security practices to mitigate the growing liability exposure from cybersecurity" (*SportsISAO*). Doug made many publications on cyber threats. Doug writes "cyber resilience and new approaches to national cybersecurity strategy" ("Douglas M. DePeppe LL.M., J.D CyberLaw Attorney & Multidisciplinary"). CRI went to sports field with Sports ISAO groups and they are finding some cyber threats in sports areas such as World Cups and Olympic games. The second research is sport articles because CRI is always posting cyber threats update in the United States in their website. As well as SportISAO is updating sport articles.

Not only does the CRI have primary and secondary sources, but they also have tools to capture cyber thieves. First, the tools that the CRI has for the c-Watch and CrowdWatch programs are threat intelligence cyber knowledge. In c-Watch, the tools that students will be using are Threat Intelligence platform, the Sport Capstone, Hands-on experience including lectures, labs, analytic frameworks and collection management (*Cyber Resilience Institute*). For example, students will learn how to spot fake news articles through social media. He or she will analyze the cyber threats and figure out where these threats are coming from. Next, the CRI uses C-Market tools to identify cyber threats. The "Cyber Market Development," states that "This project focuses on identifying the cyber risks facing small and medium-sized organizations across a variety of sectors in a certain location, spurring innovation among local vendors and businesses as the

underpinning for a sustainable model, and introducing a cyber marketplace that simplifies cybersecurity resources and adds business value for the organizations in that locality" ("Cyber Market Development Project"). C-Market will hire and pay students or a person, who have cyber security experience, to hack into someone's information and help that person protect their data by finding cyber threats on the computer.

CRI's potential of c-Watch and CrowdWatch programs to enable new modes of discovery and CI resources tools, and services in Cyber threat research that they want to decrease the cyber threats data in the future. This will help people prevent from buying new computers in order to replace their infected computer. The use of advanced CI resources, tools and services will create a better future of cyber protection.

Plans for Recruitment and Assessment

Cyber Resilience Institute has many plans for recruitment. First of all, CRI has their own website for people who have an interest in cyber security. Their website talks about their business in general, the kinds of programs they have and how to sign up for these programs. Another way the CRI gathers new members, is through students who have taken the c-Watch and CrowdWatch course. Students might tell their friends, family and/or other students about the CRI and that they recommend taking the courses if they are interested in them. The Cyber Resilience Institute's assessment is evaluating how student are going to how to catch cyber threats in the sports field.

The potential to Benefit society or advance desired societal outcomes

The potential for having c-Watch and CrowdWatch programs benefit for society is protecting everyone and their computers from cyber threat. The first benefit is that students along with people who have an interest in cyber security will learn how to capture cyber criminals. As a result, both programs help people at any age to become cyber threats hunters, and they will learn how to analysis and report cyber threats. These programs help prevent cyber threats in everyone's computers and sports events from happening again. Second benefit is information will be protected. With stronger security tools, the result will be that people do not have to buy a new computer in order to replace infected computers. CRI is willing to protect information against cyber threats and keep people safe. Overall, these two programs will benefit society.

Extent the proposed activities explore creative, original, or transformative concepts

Cyber Resilience Institute (CRI's) c-Watch and CrowdWatch programs proposed activities suggest and explore transformative concepts because the programs are cyber security base and preventing cyber thieves getting into online accounts. Since Doug DePeppe does not want the two programs as educational, but he wants to expand these programs into knowledgeable workforce for people to understand the dangers of cyber threats. It also goes with ClubWatch

where students or people can learn about cyber threats in the United States as well as internationally.

Training, education, and research workforce challenges

CRI's training, education, and research workforce are the challenges identified sound because CRI is dedicated protecting personal information along with the sports industry. Their training, education and research workforce will work together in order to help United States citizens as well as international citizens from cyber attacks.

Qualifications of the individual, team, or organization to conduct the proposed activities

c-Watch and CrowdWatch and students are qualified to conduct the proposed activities for the CRI organization. The c-Watch, CrowdWatch and the students in the programs to perform the activities will by using fundamental knowledge of cyber security. Students or members will use different cyber tools to combat against cyber threats in the c-Watch and Crowdwatch programs.

Extent the project meet its broadening access and community adoption challenges

If the CRI's projects increase in members, then they will have been successful in broadening access and adoption challenges with respect to the Nation's scientific and engineering research workforce and advanced Cyber Infrastructure by making their c-Watch and CrowdWatch available to everyone who are interested in cyber security. If the company becomes bigger then they will bring it more knowledgeable computer workforce.