University-based National Security Collaboration Center Forges Ahead

Editor's Interview with General (Retired) Guy Walsh, Executive Director National Security Collaboration Center

Many nations are experiencing a dramatic upsurge in cyber-attacks aimed at degrading security, democratic processes, and critical infrastructure systems. The ability to contend with this far-reaching challenge requires a more robust security posture than currently exists.

TE Lawrence once said, "Nine-tenths of tactics are certain, and taught in books: but the irrational tenth is like the kingfisher flashing across the pool, and that is the test of generals." The U.S. is fortunate to have a general with the adaptability, strategic mindset, and leadership qualities required to grapple with the elusive cyber-security threat.

Brigadier General (Retired) Guy Walsh is the inaugural Executive Director of the National Security Collaboration Center (NSCC) at the University of Texas at San Antonio. He leads a consortium of diverse government, industry, and academic partners working together on collaborative solutions to the national security and global defense issues. NSCC will be housed in a new state-of-the-art building (pictured below), but the organization has staked out and is implementing ambitious plans in the national cyber security space.

Walsh has had 31-year Air Force career, including 25 years as a pilot and wing commander. Following retirement, the National Security Agency (NSA) director and commander of U.S. Cyber Command chose him to operationalize cyber as the newest combat organization in the Department of Defense. His strategic vision led to the creation of Cyber Command's Guard and Reserve Directorate, where he assembled multiple partnerships and policy initiatives in collaboration with senior officials on the national security staff, Office of the Secretary of Defense, National Guard Bureau, National Governors Association, Department of

doi: 10.18278/jcip.2.1.4

Homeland Security, and Department of Justice. He was also a founding member and deputy director of the Capabilities Development group, and co-developer of CYBER GUARD, a Tier-1 level exercise to develop a "whole of nation" (federal, state, and private sector) response to cyber threats to U.S. critical infrastructure and other resources.

He was interviewed by JCIP Editor Richard Krieg in May 2021.

Krieg General Walsh, when he named you as the UTSA National Security Collaboration Center's (NSCC) founding Executive Director, UTSA President Taylor Eighmy said, "Simply put, Guy Walsh is a highly successful, highly disruptive leader whose steady hand has transformed our nation's cyber strategy ... he's the kind of leader that universities dream about recruiting." Aside from the disruption you caused providing close air support from your A-10 Thunderbolt—how would you define being a disruptive leader?

Walsh Your point is well taken; we should differentiate attributes of disruptive leadership from the disruptive nature of flying close air support missions in combat. They are very different skillsets with very different outcomes when executed properly—and very similar results when executed poorly. I would define a disruptive leader as someone who can create a common and well understood vision, communicate their intent and enable innovation and agility. Disruptive leaders are best when thinking big and empowering the team. Disruptive leaders spend much of their time thinking about the challenges. They start with problems, big problems; for example, Google's Moon Shot and Project X began by asking a variation of three basic questions: What great challenge we are trying to solve? Where are the gaps? What is it we are not doing? The decision-making process of disruptive leaders includes more time defining and detailing the challenge before jumping to solutions. Probably the most notable example of a transformational leader identifying a grand challenge began right here in Texas in 1962 when President John F. Kennedy offered America the Grand Challenge of landing a man on the moon within a decade.

Most friends and family also know and remind me that I "married up." The majority of my best decisions and successes have come from talking with my wife Ann, who has been an amazing sounding board even while I was in Afghanistan. Admittedly, I subscribe to the group that believes having a successful leadership team both at work and at

home is often more effective than flying single ship. Lennon-McCartney, Jagger-Richards, all great artists individually, but it was the chemistry that brought us the Beatles and Rolling Stones.

UTSA President Taylor Eighmy's introduction, while complimentary, is the demand signal, an expectation of deliverables and what is to come for UTSA, the National Security Collaboration Center, and the San Antonio community. Visionary leaders hire teams not based on past performance rather based on future potential. A disruptive leader lays out his vision, intent and expectations without micromanaging. General George Patton reminded his leaders: "Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity."

It is an amazing opportunity and privilege to be part of the UTSA team shaping and enabling the NSCC ecosystem.

Krieg Speaking of team building, how did your roles commanding combat operations in Afghanistan and your lead strategic role developing U.S. Cyber Command at Ft. Meade prepared you for your current position?

Walsh Team building is a universal activity and important experiential learning at any age. I encourage everyone to jump at any leadership opportunity you are offered. Whether a new Air Expeditionary Wing in Afghanistan, a new Combatant Command at Ft. Meade, or two new USAF weapons systems, there is nothing like being part of the team entrusted to design, build and mold an organization, weapons system, or a Tier 1 exercise from a blank sheet of paper. In many ways, team building in university and research institutions is just as challenging as commanding in a combat zone. Over time, team building and leadership experiences create a level of confidence and trust often based on success and coping with failure. Based on previous team building and leadership opportunities entrusted to me over the past 30 years, I can tell you that our NSCC staff and our team of federal, state, industry, National Labs, and academic partners is as capable and solid as any team in the country in addressing national security issues and building the education and workforce needed today and for years to come.

Krieg I'm struck by the scope of federal, industry, and educational partnerships that you've been able to forge at this early point in NSCC operation. How did you do that, and what is the import of this level of collaboration?

Walsh UTSA embarked on the concept of creating an ecosystem different than at any other university back in 2018, many months before my arrival. The initial effort and credit belong to the team from UTSA Research who lined up more than forty federal government and industry partners to create a new research center to advance sponsored and collaborative research. The invite to participate as an NSCC partner and work with our students and faculty researchers, if I can make a sports analogy, is equivalent of offering Super Bowl tickets to a football fan. The partnering is a win-win scenario for each partner and the University. For the partner it's the opportunity to get in on the ground floor for new business and research capacity. For the University it provides leadership of a unique ecosystem that engages with national level stakeholders and having the prospect of transforming both education, research and by enabling a diverse and qualified workforce.

In fact, industry partners such as USAA, CNF Technologies, IP Secure, and government organizations including Army Research Labs and the newly formed 16th AF had developed strong relationships with UTSA over the past five to seven years. Those relationships over time have created a trust and confidence between students, researchers, and government/industry partners. The collaborative atmosphere working in the NSCC has now brought many new innovative small companies to

San Antonio and the NSCC, working side by side with students and researchers. My favorite activity is escorting industry and government partners through our centers, institutes, and labs for the first time. I watch their eyes light up and their jaws drop as our researchers demonstrate their latest developments in artificial intelligence, augmented reality training, and human performance. Once government and industry leaders connect with UTSA students and researchers and realize the potential opportunities, my recruiting role is essentially done.

Krieg I'd like to move to the current and emerging threat environment. How would you characterize the cybersecurity threats that we currently face across critical infrastructure sectors?

Walsh The Colonial Pipeline ransomware attack this month was preceded by December 2020's SolarWinds cyberattack, also preceded by August 2019's ransomware attack against 22 Texas towns and municipalities. Cyber-attacks and exploits against our most vulnerable critical infrastructure are becoming more frequent and more disruptive. This includes government offices. The trend will likely continue as the list of threat actors continues to grow. In the context of the COVID-19 pandemic, bad actors recognized and quickly took advantage of new avenues of attack and vectors for access created by pandemic associated dependencies on a digitally connected workforce.

Having participated in the first five USCYBERCOM/DHS led exercises with our partners who own and operate U.S. critical infrastructure for the energy sector, communications sector, transportation systems sectors, and financial services sector, the threats are both significant and continuous. The sixteen U.S. critical infrastructures are under constant threat by individual criminals and nation-state advanced persistent threat (APT) actors who are backed by the governments of China, Russia, Iran, and North Korea.

Krieg Given the nature and intensity of these threats, where do opportunities exist to gain traction overcoming them?

Walsh The near-term opportunity comes from our recent first-hand experience with the loss of critical infrastructure serving our civilian and military communities in Texas. Although the culprit in this case was a natural event caused by snow and cold temperatures, the effects could have just as easily been created by a bad actor, particularly those nation state actors who have already demonstrated an ability to exploit and attack critical infrastructures including power, water, communications, and transportation.

We have to move beyond the idea that everything can be resolved with technology, a new hardware or software solution. Success requires looking beyond cybersecurity firms and software developers, it is much more complex than that as we have learned in SolarWinds.

Fundamental change to our approach will include engineers and operators, researchers, educators and policy makers. The Department of Energy's Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program is a prime example of a more inclusive approach for testing energy sector systems for cyber vulnerabilities.

If our response to resilience in the Texas power grid is to protect it from extreme weather, that would be equivalent to saying I can protect my laptop from danger by getting a new case or screen protector. We can't know which advanced attacks and techniques our adversaries will develop in the future. Assuming the adversary will always find a way into a critical system—much like the approach used by most enterprises—renders this knowledge gap almost irrelevant. The best way to manage that inherent risk lies with blocking the adversary's ability to cause the failure of a critical function, and focusing on continuity, resiliency, and the ability to operate through the crisis.

This "operate through" approach to resilience and how we engineer critical infrastructure to meet modern physical and cyber threats is an area where our ongoing collaboration with Idaho National Laboratory (INL) has proven strong. They've pioneered a consequence-driven, cyber-informed engineering (CCE) standard that acknowledges the certainty of risk and guides infrastructure owners/operators to resilient solutions.

Similarly, UTSA and NSCC's partnering with Sandia National Laboratories (SNL) is a way to make immediate impact as well as support workforce demands. Sandia has been researching the security of cyber-physical systems within our U.S. critical infrastructure since the mid-90s. Their research team here at the NSCC and in Albuquerque have the technical breadth and depth to help identify and address the underlying conditions putting our critical infrastructure at risk. Our initiatives with Sandia focus on supply chain threats, system situational awareness and resilience as well as mod/sim tools that allow systems understanding. Once we really understand the heart of these complex problems, then progress can be made on all fronts, including engineers and operators, researchers, educators, and policy makers.

Over time, critical infrastructure security will require a more balanced approach. SolarWinds, Microsoft Exchange server, and ransomware

continue to swing the pendulum on cybersecurity of business Information Technology (IT) systems. Creating more secure and resilient grids and critical infrastructure will require assessments of security and resilience measures across four threat vectors used for disruption or attack. In the use case of the electric power grid, these vectors include physical security, IT and cybersecurity, control systems/monitoring system (ICS/SCADA) security and hardening the grid against natural disasters and Electromagnetic Pulse (EMP).

Foundational components of physical security for the power grid include gates, guards, cameras and sensors. The 2013 complex attack on the PG&E power grid's Metcalf, California substation demonstrated that physical security is a cornerstone. The more recent SolarWinds and Microsoft Exchange server hacks have fueled additional research and investment on cybersecurity and the business IT networks.

While progress continues to be made in areas such as zero-trust environments, securing the business IT system is not enough and can create a false sense of security. Locking the front door is an important step; however, we cannot ignore the open windows and garage door. In the case of our critical infrastructure and electrical grid, additional R&D and investment is needed for securing control systems, the operational technology (OT) systems, and the monitoring systems including ICS/SCADA, the third vector.

The *Journal of Critical Infrastructure Policy's* control systems article by Joe Weiss in your 2020 Fall/Winter edition provided great insight to these vectors not being addressed for business IT systems. Published research by another engineer, Mike Swearingen, resulted in a thought-provoking IEEE paper on an autonomous, self-aware, smart grid framework. Both provide important perspectives from engineers, plant operator communities. For too long, attention to monitoring systems and control systems security has been ignored or overlooked. Protecting the federal enterprise and the nation's critical infrastructure is about a balanced approach to securing business IT systems and control systems security and resilience.

The fourth vector, best described as the worst-case scenario, is protecting the electrical grid against an Electromagnetic Pulse (EMP) event such as a solar flare or nuclear detonation. Coming from a military background, we always planned for both the most likely scenario and the worst-case scenario. To address the EMP threat, our NSCC has been fortunate to team with organizations including Joint Base San Antonio, the City of San Antonio, Southwest Research Institute and CPS

Energy to create the San Antonio Electromagnetic Defense Initiative (SAEMD). Led by NSCC Technology officer, Dr. John Huggins, JBSA's Mike Lovell, Dr. Patricia Geppert and LtCol (ret) Steve Chill, SAEMD enables research and collaboration among the San Antonio and Alamo Region communities and our military partners to locally implement the USAF Electromagnetic Defense Task Force recommendations.

The mission statement of the SAEMD Initiative is to "educate, collaborate, and facilitate domestic electromagnetic spectrum operations (DEMSO)." Where military EMSO is focused on spectrum dominance, DEMSO is focused on homeland survivability and resiliency. More precisely, DEMSO comprise those activities to normalize, enable, and sustain commerce and comfort as modern society becomes increasingly reliant on the electromagnetic spectrum with awareness of electromagnetic pulse risks through policy and education.

Krieg From my perspective, one of the more exciting and newest components of the NSCC ecosystem is the Department of Energy's Cybersecurity Manufacturing Innovation Institute (CyManII). What is it and how does it operate?

Walsh The Institute is one of the biggest wins for UTSA, San Antonio, and the State of Texas in this century. It starts with understanding the problem statement. U.S. Manufacturing is the number one target for nation-state cyber-attacks against our country. As manufacturers implement digital transformation throughout their supply chains and production pro-

cesses, they exponentially expand their cyberattack surfaces. Thus, innovation and modernization of U.S. manufacturing can be compromised by inadequate cybersecurity defensive measures. We need a game-changing approach. CyManII delivers this game changer.

Dr. Howard Grimes, CyManII's CEO, has assembled an all-star team that will develop and introduce the "smart manufacturing architecture" or SMA. This open architecture will combine the physical, cyber and energy layers in manufacturing systems. The SMA introduces: 1) a secure by design architecture, 2) cyber-physical passport that creates a supply chain that is rooted in trust, and 3) a mechanism to capture every energy transaction. Together, these will allow U.S. manufacturers to invest in cybersecurity innovations because it protects their designs and significantly increases their energy productivity.

The SMA will work with both legacy systems as well as the most advanced technologies used by manufacturers. CyManII's "north star" is to introduce a game-changing secure manufacturing architecture that is energy efficient, pervasive, unobtrusive, resilient, and economical (ε-PURE). CyManII will also launch a work force development program that will upskill SMMs and OEMs workers in state-of-the-art cybersecurity practices and in the optimization of SMA for resilient operations. By using the SMA, and other innovations that CyManII will roll-out, U.S. manufacturers will be globally competitive for decades. CyManII is a great win for Texas and the Nation.

Krieg What are the other research components that will be lodged within NSCC, and how does that relate to the NSCC's work with the National Laboratories?

Walsh The UTSA NSCC has established cooperative research agreements with Idaho National Laboratory in the area of energy and electrical grid sector resilience, now carrying more significance for Texas due to the recent winter storm. With Sandia National Labs in Albuquerque, New Mexico, the research focus has included cyber-physical and hardware security. Most recently we have been collaborating with Pacific Northwest National Labs (PNN) in Washington state in the areas of 5G communications. One of the more notable research partners is located here in San Antonio, Texas, our very own Southwest Research Institute (SwRI). SwRI President Adam Hamilton, and the 3,000+ researchers and engineers, are a cornerstone of innovation for Texas. The Institute is known for applied research and helping develop world-class solutions, from 'Liquid Paper' to components used on NASA's Mars rover.

It is interesting to me that SwRI was established in 1947, the same year our U.S. Air Force was established.

For the past two years, the UTSA NSCC has also partnered with the MITRE Corporation, a Federally Funded Research and Development Center (FFRDC) that created the Generation AI Nexus, a curriculum integration providing students access to AI training, tools, and big data. Of the dozen or so initiatives with MITRE, one recent effort involves the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and our Center for Infrastructure Assurance and Security (CIAS) to provide assessment and cybersecurity preparedness to 15 participating Texas and San Antonio non-profit and faith-based organizations. Student teams, MITRE mentors and the participant's technical support will work together to establish a more resilient computer network environment. One outcome of this initiative will define the scalability protocols for a nation-wide rollout in coordination with DHS and CIAS.

The NSCC frequently communicates through video conferencing with University Affiliated Research Centers (UARCs) to stay connected and informed on multi-institutional research opportunities such as telehealth and telemedicine. The relationships with the national labs, FFRDCs, and UARCs have contributed to UTSA and the NSCC being recognized by the Department of Defense, Department of Justice, the Department of Homeland Security, and the Office of the Director of National Intelligence as an up-and-coming research center. More importantly, UTSA is recognized as the nation's top Minority Serving Institution and Hispanic Serving Institution that enables a more diverse cyber-ready workforce.

Krieg Cybersecurity concerns include—but are not limited to—financially motivated attacks from organized crime, insider threats, activists or "hacktivists," and nation-state actors. Cyber attacks from national adversaries should arguably be the biggest concern. In broad strokes, how can we fully engage that issue? Also, in your view, is the right leadership team in place in Washington and the Pentagon-Ft Meade to create outcomes?

Walsh As a former A-10 Close Air Support pilot, I was most comfortable in being down in the trenches and in the weeds; however, in this case, taking a 50,000 ft view of existing and emerging threats and of our leadership team creating national intent is a sounder approach. Full engagement in broad brushstrokes requires leadership across the federal government and U.S industry, what we referred to as the Whole-

of-Nation approach. Do we have the right set of "Disruptive" leaders in place in Washington, D.C. to move the needle: I will argue a resounding "Yes."

In June, the U.S. Senate unanimously approved the nomination of Chris Inglis as the nation's first national cyber director as recommended by the Cyberspace Solarium Commission (CSC). Serving as a bridge between the White House and Congress on cybersecurity matters, the creation of the cyber czar represents a major step toward establishing a Whole-of-Government and Whole-of-Nation approach. Inglis brings over forty years of continuous military and senior executive service to the table, serving as NSA's Deputy Director more than twice as long as the average tenure of three years across NSA's 70-year history.

Chris was a steady voice on the CSC, which recently provided roadmaps and recommendations to the Biden administration. The CSC white paper describes three processes that will elevate cybersecurity across the government and put the United States on a path toward reducing the probability and impact of cyberattacks. The CSC report lays out seven operational priorities and promotes a positive legislative agenda for cybersecurity that expands beyond prevention to resiliency.

At Fort Meade, I was fortunate to serve with U.S. Cyber Command during its first decade as a new Command. I would offer both DoD and the Intelligence Community had the right leaders at the right time, each addressing a unique set of challenges: General Keith Alexander, created a new Combatant Command outlining a strategic plan, establishing an organizational structure that leveraged its reserve component and industry partners; Admiral Mike Rogers, operational lead charged with a mission to organize, train and equip the nation's 133 team cyber mission force and achieving fully operational combat capability in rapid order; and General Paul Nakasone, given new authorities to execute a defend forward, secure the electoral process against nation state interference via a policy of persistent engagement. In sequence, their vision and determination changed the culture from supporting military operations to becoming operational warfighters. Each understood the importance of building trust and confident partnerships with federal agencies, close allies and critical infrastructure industry, into the training and exercises, building trust and confidence and creating outcomes.

There is something to be said for having leaders who are involved in the strategy process also leading the path for implementing and executing laws that protect our civil liberties while engaging with adversaries.

Adding his vision, tenacity, and team approach, I am very optimistic regarding nominations of Chris Inglis and Jen Easterly to White House Cybersecurity and DHS Cybersecurity and Infrastructure Security Agency (CISA) respectively. Having worked our way through policy, roles and responsibility and legal challenges early in the establishment of DHS, CISA, and USCYBERCOM, the whole of government lineup with both Anne Neuberger, deputy national security advisor for the White House, and Rob Joyce, director of the NSA Cyber Security Division (CSD), have already demonstrated strong chemistry in previous roles. Like establishing U.S. Cyber Command, the addition of a National Cybersecurity Director will not happen overnight; however, we are in this for the long haul as is our new leadership team.

Importantly, the National Security Council (NSC) role is about establishing National Priorities. Having a strong leadership team from the top down is one third of the road to success. Political analyst Graham Allison described the influences of the rationale actor model in his book *Essence of Decision,* which highlighted the impact of the organizational model and the influences of political bureaucracy that has a life of its own, independent of the leader in charge. I look forward to the upcoming discussion on roles, responsibilities and the challenges of aligning authorities with the resources and capacity to scale. I believe that will be key to determining success in building resilience and a competitive edge.

The role of the National Security Council (NSC) is setting national strategy, policy and priorities and the role of Department of Homeland Security/CISA is protecting critical infrastructure, disseminating threat information and best practices—education and training. It will be interesting to see how the administration leverages and empowers the position of a new national cybersecurity director (NCD). Will the NCD be able to execute and operationalize national priorities not only across federal government but create outcomes and capabilities for response, prevention and resilience aligned with state, local and critical infrastructure industry partners for a much-needed Whole-of-Nation approach to overcome current and emerging cybersecurity threats?

Krieg Last question. As you look forward, General, what is your vision of NSCC 5 years from now?

Walsh I tend to work backwards in time and would offer that San Antonio and the UTSA NSCC vision over the next two to three decades should be to be creating the next "Silicon Valley," with innovation matched with a much greater emphasis on the human capital and leveraging the diver-

sity of our Texas population to meet and exceed the gaps in education, research and workforce development. If we see that as San Antonio and Texas' vision, we can now back up to the 5-year increments and 10-year mark and ask what needs to be in place in 2025 and in 2030 to achieve an end state in 2040.

Let's start with a simple problem statement as an example: Are we providing an end user, an operator, a controls system engineer, a plant manager or a warfighter with the tools they need to do their job. The NSCC ecosystem brings together a transdisciplinary team that includes professors, researchers, and students, side by side with federal and industry partners and end users /operators. San Antonio and Joint Base San Antonio are leading major pilots and experimentation for the Department of Defense in 5G integration, telehealth and telemedicine, and resilience of the energy grid against worse case events including solar flare and electromagnetic pulse threats. UTSA and the NSCC will play a major role which is great for our economy and will provide tremendous opportunities for future generations here in Texas.

Success will come as we dispel a misconception that university research centers and institutes are only able to provide foundational research. Experiential learning and exposure to applied research and innovation is precisely what is needed to tackle the growing gap in our digital workforce. Federal and industry partners bring with them much needed applied science and engineering. Introducing more of the applied sciences needed in the field makes for much better graduates and workforce at both the undergraduate as well as graduate level education.

Both high schools and higher education appreciate not only key foundational research but also higher Technology Readiness levels. There is tremendous interest in UTSA's transdisciplinary approach to education and research.

In assessing the San Antonio and Austin Texas region, all of the key ingredients for success were in place. Strong academic institutions many with strong focus on STEM engineering, data analytics, emerging areas of AI, Quantum, hypersonics, and digital manufacturing. One key ingredient unique to San Antonio is the diverse federal government presence. The same government organizations that created the demand signal at Stanford University and Silicon Valley seventy years ago. Bringing in academia has two major effects to address gaps in the workforce and education. Most forward leading universities are focused on addressing the national security challenges.

To be truthful, the vision is where the City of San Antonio and Texas will be by 2030, not only exceeding the San Antonio ecosystem, but securing and building resilient energy grids across the globe.

Leading 5G integration and experimentation for DoD also means tackling San Antonio's digital divide within the next five years. How can we say we will lead change around the globe without first fixing our own backyard? Building upon 5G and the follow-on 6th generation telecommunications technologies of increased bandwidth, low latency and segmentation to, for example, securely perform intricate surgery remotely anywhere on the planet, crowdsourcing a team of doctors on different continents through augmented and virtual reality. Today, these same procedures can only be performed by a handful of small teams at just a few medical centers around the world. San Antonio and the UTSA NSCC will be at the heart of creating a secure and much more resilient internet for future generations leveraging artificial intelligence, quantum computing, and—just as the semi-conductor brought success to California—the UTSA NSCC and CyManII will bring the U.S. back to the forefront in manufacturing and building products once again.

Looks like we have our work cut out for us and what can be more exciting than that?