INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

CONVERGENCE OF MISSION AND MOMENT:

IMAGINING THE EMERGING TECHNOLOGY ANALYST

Institute for Homeland Security

Sam Houston State University

Nick Reese

CONVERGENCE OF MISSION AND MOMENT

Imagining the Emerging Technology Analyst

Nick Reese *Triantha | nickreese87@icloud.com*

Abstract

The Department of Homeland Security (DHS) was built to prevent terror attacks in the homeland and its culture and structure reflect its birth in 2002. Unlike the world changing event that created DHS, the gradual fading of the terror threat has left it misaligned to respond to new nation-state sponsored threats. The homeland security mission is at a true inflection point as it looks for new ways to use its capabilities and authorities while the central force driving global competition is being established. Just as the field of cyber was being established in the late 1990s and early 2000s in response to new threats, so too must the field of emerging technology be developed today. Examining the realities of the world today, we see the need for professionals who specialize in how emerging technologies create risks and opportunities in a way that is distinct from how cyber professionals do the same for the cyber domain. This work examines the geopolitical reality and how it reflects on the homeland. It goes a step further by conducting a comparative analysis between current cyber analyst requirements and skills and what would be required for an equivalent emerging technology analyst. This analysis informs governments, academia, and industry by creating a baseline from which emerging technology professionals can be created and evaluated with direct application on practitioners in critical infrastructure.

Introduction

The Department of Homeland Security (DHS) was born in a different time. One year, two months, and twenty-four days after the attack on the World Trade Center, Pentagon, and United Flight 93, DHS was born. The Homeland Security Act was signed on November 25, 2002, and carried with it fresh and open wounds from the horrifying attack just over a year past. The authorities granted to the new Department, its Components, and its eager workforce were all shaped by the new geopolitical era that would come to be defined by non-state actors. First responders, critical infrastructure, and industry all followed the lead of the founding of DHS and focused intensely on the prevention of attacks. Another wave of terrorist attacks on U.S. soil was assumed and lawmakers and policy makers marshalled funds and resources to provide the tools homeland security organizations needed for the fight. For the next twenty years, the homeland security mission would be defined by the manner of its birth; secure the homeland against the terrorist threat.

That was then. Still a threat but not nearly with the power and reach to dominate geopolitics, the era of non-state actors such as al-Qaeda, Daesh, and al-Shabab has faded into the shadow of the new era. Unlike the world changing event that created DHS, the gradual fading of the terror threat has left it misaligned to respond to new nation-state sponsored threats. A series of five-year plans and clockwork eight percent per year economic growth placed China in a position with a new term in geopolitics; near-peer adversary. Bringing small-economied but likeminded allies along, China created the beginning of a geopolitical orbit not seen since Cold Warera capitalism versus communism. National powers around the world are all arriving at the same conclusion at the same time, emerging technology is the source of power of the future.

Technology has been a primary feature of statecraft since the Greeks built defensive walls around Athens in 465 B.C. E. catalyzing the Peloponnesian War. However, today's race centers around technological advancements that dwarf others in the history of statecraft. Artificial intelligence (AI), quantum information science (QIS), new infrastructure for soft power, biotechnology, advanced materials, space capabilities, and other technologies are central to the Chinese plan for usurpation of the U.S. position as the dominant economy and dominant power in the world. A new era of great power competition has begun, and the quantity being competed over is emerging technology and all that supports it.

This paper studies the convergence of two inflection points, the shift of the homeland security mission and the maturation of emerging technology as a defined professional field. This moment in the history of homeland security in the U.S. is one that will be looked back upon and studied as two extraordinary factors are colliding to create the conditions for a new way to define the practice of homeland security. Just as cybersecurity was a new field 30 years ago, so too is emerging technology today. Emerging technology's maturation parallels the trajectory of the homeland security mission provided organizations can identify the global dynamics that will affect them soon. Cyber is the domain where this competition is taking place, but it is not the goal. Global dynamics show us that the goals of our adversaries surround emerging technology and that technology is primarily being developed in the private sector. That means the private sector is the target of cyber actors with nation-state resources behind them who are in pursuit of their most valuable intellectual property. Intellectual property that will be applied to adversarial actions against the homeland. To meet this moment, this study will build the first vision of an emerging technology analyst to help governments, academia, and industry define this new role and the skills required to make impact in this new reality.

Structure and Context

A brief examination of world power dynamics over the last seventy years reveals three significant shifts in the dominant threats to U.S. interests. Post-World War II (WWII), the Cold War era was characterized by a bipolar world with two dominant global powers competing for hegemony.[1] Globally, smaller, less powerful states were pulled into either the capitalism or communism orbit. This competition over economic systems and systems of government created a global arms race that developed into an existential threat to life on earth. The fall of the Soviet Union in 1991 left the U.S. as the unrivaled global hegemon in an era that would soon be defined by the rise of non-state actors.[2] September 11, 2001, brought a world changing event that pivoted the world's attention to the terrorist threat and defined the practice of homeland security for twenty years. Twenty years of war against terrorism diminished the role of non-state actors in global power dynamics. The era of non-state actors was characterized by ideologically motivated irregular warfare that included a broad sense of good versus evil, making it a compatible issue internationally. Traditional non-allies were happy to collaborate on counterterrorism issues because it was a zero-sum game with little sympathy for terrorist causes and considerable international consequences for lending support. In each of these constructs, the issues of the day drove the application of state power, which in turn drove priorities, budgets, missions, and more. Terms like "national security" or "homeland security" or "economic power" meant measurably different things in different eras because of the geopolitical context. With the benefit of hindsight, we can look at our current era and place a theoretical framework around it to give decision makers the advantage of having the structure and context to make the right decisions.

State power is an elusive term in international relations and is generally understood as the ability of one state to bend the will of another state to take an action it would not otherwise take. Instruments of power in traditional statecraft levers may include military, diplomatic, economic, financial, law enforcement, and others. States also practice soft power such as influence, international institutions, culture, etc. In the context of GPC, power refers to a state's ability to develop its own statecraft-level technological capabilities and its ability to effectively employ them. Even with significantly larger economies, 2nd and 11th, respectively, China and Russia are in no hurry to engage in a force-on-force hot war with the U.S. and the North Atlantic Treaty Organization (NATO) but are constantly exerting power through cyber-attacks and pouring treasure into the development of emerging technologies such as AI and QIS.[3] As these countries continue to sponsor technological development at a state level and continue to refine their craft, they present a real threat to critical infrastructure, democratic institutions, data privacy, military secrets, intelligence methods, border security, and more. Holding one's water supply system hostage by infiltrating its operational technology systems is certainly a way to bend the will of an adversary to take an action it otherwise would not.

The current GPC era competition is over emerging technologies and the standards and norms of their development and use. Exercising state power is now a function of a state's ability to develop and employ technology to attain hard power goals, such as cyber-attacks, or to

---

[1] Thies, Cameron; *The Roles of Bipolarity: A Role Theoretic Understanding of the Effects of Ideas and Material Factors on the Cold War*; August 2013; International Studies Perspectives, 14 (3), pp 269-288; Oxford University Press

[2] Krauthammer, Charles; *The Unipolar Moment*; January 1, 1990; Foreign Affairs; https://www.foreignaffairs.com/articles/1990-01-01/unipolar-moment

[3] Silver, Caleb; *The Top 25 Economies in the World*; September 1, 2022; Investopedia; https://www.investopedia.com/insights/worlds-top-economies/

increase its economic footprint in support of soft power goals. Emerging technology is the commodity over which states will compete and around which state power will be defined. Within emerging technology are essential elements that a state must control in order to be considered a great power. Being a great power in the GPC era means having a strong and attractive innovation ecosystem. Defining this ecosystem gives homeland security professionals both a list of strategic assets that must be protected and a list of targets an adversary might strike. The innovation ecosystem and its strategic importance definitively shift more burden onto the homeland security mission space than in previous eras. Global competition surrounds emerging technology and emerging technology is developed inside a nation's innovation ecosystem. That innovation ecosystem is the target of disruption and intellectual property theft by adversary nation-states and those actions are taking place inside the homeland. It impacts our critical infrastructure, economic progress, and our top talent. However, if homeland security professionals are to understand what they are protecting, we must define the essential elements of a strong innovation ecosystem; digital creative industries (DCI), advanced materials, strategic investments, and standards and norms.

DCI

A space currently dominated by the U.S., DCI is the industry that creates social media, multimedia platforms, gaming, popular applications, hardware, and other online entertainment. DCI is a critical element because it is the engine that generates the economic value that is then pumped back into the R&D cycle creating new innovations and more economic value. The products of DCI such as social media platforms, mobile devices, and online streaming services provide the infrastructure on which American soft power is delivered to the world. Those same products represent the platforms on which American offensive cyber capabilities occur and where intelligence collection activities reside. The loss of American dominance in DCI means the loss of a soft power dissemination, control over the cyber battlespace, and the loss of intelligence collection capabilities.

Materials

Continued innovation depends on the availability and production of advanced materials such as new alloys, semiconductors, and lighter carbon materials. The production of advanced materials in turn depends on a complex supply chain that includes the mining of rare earth minerals and possible mining efforts in outer space. Semiconductors are the most ubiquitous and best-known example of the need for advanced materials and the importance of their supply chain. China has already taken significant leaps forward in their domestic semiconductor production, threatening the market share of American companies such as Intel.

Strategic Investment

DCI companies such as Google are involved in the development of new and groundbreaking technologies that have nothing to do with their core business of search engines, social media platforms, or gaming. Google invests significant resources and treasure into biomedical research that may result in extending human life. Google and others are investing strategically to make breakthroughs that will become their core business in the next decade and beyond. They are looking beyond their current economic value and planning for the next innovation that can create and dominate a new market first. Strategic investment should find ways to support emerging technology research with mutual benefit to private companies and the government without crossing the line of state-controlled enterprises like Russia or China.

Standards and Norms

Much like air power in World War I, cyber power in the first decades of the 2000s, and space in 2020, emerging technology is an area where standard and norms are being defined with implications to state power. How standards and norms develop could result in the migration of technology companies and talent to one market over another. In May 2023, the U.S. government published its first ever National Standards Strategy prioritizing U.S. participation in international standards making processes for critical and emerging technology.[4] This document is a strategic move to position the U.S., and its innovation ecosystem, in a leadership position in standards making.

Putting emerging technology into the right context and defining its critical elements are important first steps. The largest players in the elements of the innovation ecosystem above are in the private sector but their actions have direct impacts on homeland security. The nexus between private sector technology development is a significant feature of a future emerging technology analyst and of the emerging technology field. To build on this understanding, we will move to a comparative analysis of the homeland security mission and emerging technology as a driver of global action.

Convergence

We reviewed the manner of the birth of DHS, the September 11, 2001, terror attacks. We see how a world changing event created a new U.S. federal government department and how the broader field of homeland security followed the cultural and organizational lead of its establishment. The homeland security mission space was dominated for over 20 years by the fight against terrorism as the major elements of U.S. national power were focused on the terrorism issue at home and abroad. During that same time, the cyberspace emerged as a contested domain for terrorists, nation-states, and criminals alike. Social media, online gaming, and other online communications also proliferated during the same period. While homeland security organizations focused on detecting explosives on aircraft and stopping plots against domestic targets, the nation-state threat was beginning to emerge in the cyber domain. New capabilities were being developed to attack adversaries in new ways. Ways that allowed for direct attacks on home soil that have not been possible without an invading army in previous generations. Homeland security organizations were certainly not blind to the threat but the context around it would not become clear until much later.

As cyberspace became a contested domain internationally, the world's powers devolved into a constant state of cyber warfare where attacks, disruptions, and persistent presences have become a daily occurrence. Cyber-attacks are not merely launched as an augment to a traditional conflict but used constantly in what USCYBERCOM calls "defend forward."[5] This constant state of cyberwar developed slowly over time into a defining characteristic of this geopolitical era. Rather than being able to point to one or two defining events such as the fall of the Berlin Wall or the September 11th attacks, two slow burn factors came together to create the dynamics that are changing the homeland security mission. First, twenty years of sustained global pressure

---

[4] The White House; *National Standards Strategy for Critical and Emerging Technology*; May 2023; https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf

[5] Goldsmith, Jack; *The United States' Defend Forward Strategy: A Comprehensive Legal Assessment*; March 2022, The Hoover Institute; https://www.hoover.org/research/united-states-defend-forward-cyber-strategy-comprehensivelegal-assessment

eroded the power and reach of the international terrorist groups that carried out complex and multinational attacks. Second, the cyber domain was maturing and with it the professionals that would specialize in cyber. Cyberspace is a contested domain, but it is the means by which other goals are achieved in the same way that control of the air domain helps militaries achieve their goals. Cyber is an attractive method to launch action against an adversary because it is cheap and offers some degree of anonymity. The question that should be asked is not about why or how the cyber domain is being used but what the goals of its use are.

The decrescendo of international terrorist organizations and the crescendo of cyber warfare slowly be definitively changed what is meant by national security and homeland security from the era prior. By the early 2020s it was clear that cyber threats to both information technology (IT) and operational technology (OT) were significant threat vectors and attacks against critical infrastructure by these means could have catastrophic effects on the homeland and the economy. At the same time, scientific and technological breakthroughs were growing new capabilities in emerging technologies like AI, quantum, telecommunications, data, and outer space. Nation-states around the world, including the United States, recognized the strategic advantages conferred upon the state that can bring these capabilities both to the economic market and into their state power arsenals. The nexus with the constant state of cyber warfare was immediately apparent in that states could both augment their cyber capabilities and use the cyber domain to augment their emerging technology capabilities. States could steal intellectual property from an adversary's innovation ecosystem at home to shortcut their own research and development projects. They could likewise outsmart cyber defenses or engage in increasingly effective information operations by bringing technologies like AI to bear. As of 2023, this dynamic is now the one that dominates interactions between adversaries in the cyber domain.

Cyber is a domain but is not itself a goal. Cyber is the "how" but the "what" is equally important. Nation-state conflict and competition increasingly takes place online, but those operations are being done with goals in mind. A review of national priorities around the world over the past three years nets thousands of pages of policy documentation prioritizing emerging technology strategic advantage. As one example, the U.S. signed the Initiative for Critical and Emerging Technologies with a strategically important partner in India using emerging technology as an internationally compatible issue in the same way that counterterrorism was once used.[6] China's Made in China 2025 plan prioritizes an intelligent Industry 4.0 vision, which would require dominance in areas like Internet of Things (IoT), telecommunications, AI, cloud computing, and more.[7] In 2017, Russian president Vladimir Putin said that the country that leads in AI will be the leader of the world.[8] Many more laws, Executive Orders, policies, and priority documents can be found that say the same thing; major powers around the world are prioritizing

---

[6] White House; *United States and India Elevate Strategic Partnership with the initiative on Critical and Emerging Technology*; January 31, 2023; https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/31/factsheet-united-states-and-india-elevate-strategic-partnership-with-the-initiative-on-critical-and-emerging-technologyicet/

[7] Kennedy, Scott; *Made in China 2025*; June 1, 2015, CSIS; https://www.csis.org/analysis/made-china-2025

[8] Maggio, Edoardo; *Putin Believes that Whatever Country has the Best AI will be "the Ruler of the World"*; September 4, 2017; Business Insider; https://www.businessinsider.com/putin-believes-country-with-best-ai-ruler-ofthe-world-2017-9?op=1

emerging technologies. With well-developed cyber capabilities and professionals, the cyber domain was the logical place for competition to start and it has been playing out this way since.

This convergence of events creates an entirely new mission dynamic of homeland security organizations across the country and for the professionals that support them. If the development and ultimate leadership in emerging technologies is the stated goal of the world's powers and they are using the cyber domain to execute on their priorities, that means that nationstate actions will by nature take place against targets inside the homeland security mission space. Homeland security professionals must contend with threats that have nation-state level resources and a recognition that targets like critical infrastructure services are legitimate. Success in a newly defined homeland security mission space means first recognizing the shift then bringing existing capabilities and authorities into alignment with contextual realities. The contextual reality that created DHS and rapidly expanded the homeland security mission continues to define its culture today. However, we are in a moment where two slow burning changes have reached inflection points and attention is required. A new professional that can cut across domain expertise and technical expertise and can view risk based on the correct geopolitical context.

Building the Emerging Technology Analyst

This study thus far has focused on the change in geopolitical era and its impact on the security of the homeland, however, this perspective is not the primary focus of the paper. Whether felt directly or as a second or third order effect, the characteristics of any geopolitical era impact governments, private companies, and academic institutions alike. Universities respond to global conditions by offering new programs of study that reflect the needs of public and private employers. Governments respond through budget prioritization, creation of new offices, and adjustments to missions sets. Private companies respond by protecting their interests and offering products and services that reflect the needs of others. Central to all of these responses is the people that each organization brings in to lead their response efforts. This dynamic has been on full display over the past twenty years as organizations, public and private, have brought in cyber professionals and universities have increased their cyber-based offerings. While this response has absolutely been warranted, it has only addressed part of the problem.

Cybersecurity will continue to be an extremely important aspect for public, private, and academic organizations and the demand for cyber professionals will remain. What has been missed is that cyber is not a goal. Cyber is a means that nation-states and cyber criminals use to achieve their goal. Cyber's value proposition is that it allows one to infiltrate otherwise sovereign territory and escape with something valuable with a reasonable chance of not being caught or attributed. That's tremendously appealing but only insofar as it yields something of value. Per multiple strategic documents from multiple world power, that something valuable is emerging technology in the form of intellectual property, data, and source code. In the U.S., and in fact in most of the Western world, the value being created in the emerging technology domain is being created by the private sector making it the target for cyber operations with nation-state resources behind them. Many private companies are not equipped to withstand attacks that are funded and resourced by a nation-state government, but they find themselves in the crosshairs. This problem has no singular solution but a part of it is the development of emerging technology as a professional field in the same way that cyber developed over the last thirty years.

Augmenting the technical cybersecurity expertise with emerging technology expertise will create a strong team that is trained in both the technical defenses and recognizing the targets before the attack.

Before we think about an emerging technology analyst, we will define the emerging technology professional field. Much like any professional field, there will be areas of specialization and focus but the following characteristics will be critical based on the analysis above.

- STEM/National Security Blend: An emerging technology analyst should have a deep STEM background enabling them to be conversant with technologists developing the technologies. Likewise, the analyst should be able to recognize geopolitical factors that may impact emerging technology development or implementation. This crossover will require an equal blend in terms of depth and complexity in both fields.
- Public/Private Sector: An emerging technology professional should as a matter of professional development spend time in both the private and public sectors. This will help bridge the gap that characterizes public-private cooperation on technology.
- Tactical and Strategic: Emerging technology analysts should be able to recognize how the strategic situation impacts day-to-day missions on the ground. Having direct impact that can be felt by practitioners should be the goal.

The government needs professionals like this to make effective technology and national security policy decisions on critical technology topics. The private sector needs these professionals to identify the targets of significant cyber-attacks to give defenders a real chance to withstand attacks. The question is if an organization will be attacked but its ability to recover. Recovery is important but the emerging technology professional can have impact to the left of the event and help reduce the damage and lessen recovery time. This provides immediate value to private companies who are targets every day. The bridge between the public and private sectors also provides instant value to sides.

Importantly, most strategic national assets in recent decades have been about power projection. Think aircraft carriers, intercontinental ballistic missiles, and long-range bombers. Today, we are adding another strategic asset that by its definition is in the homeland and directly includes private technology firms. The innovation ecosystem is the most valuable strategic asset for the U.S., and it resides inside the homeland. Unlike the traditional view of strategic assets as power projection, the innovation ecosystem is the base from which the U.S. with derive its power for decades to come. In another shift, this strategic asset focuses on the private sector and academic institutions. The crossing of national security and private innovation is the defining characteristic of this geopolitical era and organizations, public and private, need professionals trained to meet this challenge.

CYBER ANALYST EVOLUTION

The cyber analyst position has been around long enough to have gone through a few evolutionary cycles. Appendix A contains two sample job descriptions from major federal government contractors for a cyber analyst and a threat hunting analyst, respectively. In each, education requirements can be offset by years of experience. Both descriptions show the willingness to hire a candidate with only a high school diploma if that person meets the requisite number of years of experience. Certifications of skills like coding, network security, and others

are also listed as primary qualifications along with the ability to obtain and maintain a security clearance. Cyber is evolving this way because the skills required to be a cyber analyst can be learned through a variety of means including, but not limited to, formal degree programs. A cyber analyst is becoming a very skills-based profession requiring constant upskilling and updating of current approaches that can be done as a part of a formal study program or within online communities. While traditional degrees in the subject are offered and undertaken by prospective cyber analysts, there are other approaches, and some may decide not to invest in the degree program given the requirements. Cyber analysts are highly technical and specific often with deep expertise in certain types of systems, coding languages, or aspects of cybersecurity.

The field has had time to mature into these highly specific sub-topic areas allowing for greater specialization. An academic institution seeking to serve the needs of cyber analyst professionals must contend with the reality that employers are not necessarily requiring traditional degrees to obtain a well-paying cyber analyst position. The market for cyber skills certification is saturated with companies and certifications that are accepted as the industry standard. Some will choose the traditional route, but others will choose not to incur the costs and spend the same years working to increase years of experience. The skills and experience required to be an effective cyber analyst are well known and accepted across the industry preferencing highly specific skills development and experience at least on par with formal degrees.

Building the Emerging Technology Analyst

The nature of emerging technology as a geopolitical reality demands a different approach for developing professionals. Being a highly specific professional in a single emerging technology area such as AI or quantum is not sufficient. It is also not sufficient for a prospective professional to have the "mile wide, inch deep" approach because understanding the impacts of emerging technologies in various critical infrastructure and homeland security mission areas requires technical knowledge.

As emerging technology matures as a professional and academic field, its definition may change but can at this moment be generally characterized as the study of the impacts of emerging technology research, development, deployment, and implementation on a given mission area.

To affect this outcome, an analyst would have to undertake a significantly different training and continuing education program than a cyber analyst; one that is more conducive to the offerings of academia.

The emerging technology analyst possess a broad base of knowledge but also have enough depth in each to be able to both explain technical topics to non-technical audiences and to evaluate technical details of technology development for their impacts to given mission areas. In this way, the emerging technology analyst requires a knowledge of international relations, advanced mathematics, computer science, physics, sociology, crisis communications, and public policy. The analyst would be required to interface with technical experts and developers, nontechnical decision makers, cyber professionals, and academics among others. It is not possible to achieve this with a pure generalist approach but to overlap more heavily with STEM courses and learning. Much like cyber, emerging technologies evolve and change rapidly making the need for continuing education critical. As such, the following is proposed as a framework for emerging technology education in upper division undergraduate requirements and post-graduate work augmented by professional development training courses:

A. Courses in Domain Specialty
    a. Energy
    b. Law Enforcement
    c. Healthcare
    d. Others
B. Courses in Technical Skills
    a. Mathematics (linear algebra, calculus, etc.)
    b. Computer Science
    c. Data Science
    d. Physics
    e. Biology

This course work should be followed up with a for-credit practicum that provides students with scenario-based practical application of the skills they learned.
Professional development courses should be curated over the life of the student's career and provide updates in specific technology areas of strategic importance paired with leadership and organizational management courses:

A. Quantum
B. Blockchain
C. AI
D. Outer Space
E. Telecommunications
F. Organizational Change Management
G. First Line Leadership
H. Budget Management
I. Others

Together, these courses create a consistently relevant path for student success and the continued security of the homeland.

Whereas the skill and education requirements for cyber professionals is trending away from the formal academic institution models, the emerging technology field is by its nature suited for direct and long-lasting engagement between academic institutions and learners. Creating a new model whereby the graduation of a student is not the end of their engagement with the university, but the beginning creates a constant resource for students and a constant source of revenue for academic institutions. Creating both undergraduate and graduate programs that combine domain expertise with technical knowledge will serve students and the homeland by focusing deep skills and understanding. After graduation, academic institutions should create a talent pipeline that offers a variety of professional development and upskilling programs tailored to the working professional and aligned with specific career phases. In this way, academia can maintain relevance in a new technical field rather than seeing its phasing out as is taking place in the cyber profession. Engagement with the community through events and unique research will augment this approach and create a sustained leadership position attracting students and life-long learners alike. This presents an opportunity for first movers in academia to establish themselves destinations of choice for domain experts to continue their education and create the critical mass of enrollments required to sustain an emerging technology program.

Recommendations

The creation of a new academic and professional discipline is not a simple undertaking and often lags the real-world need. Cyber had to grow and develop into the field it is today but that process has been slow. We are already in a world that demands emerging technology professionals, but defined career paths and training programs are lacking. In order to affect a more expeditious path to value for private and public organizations, the following recommendations are provided. These recommendations target private companies and academic institutions and serve as actions that can be taken immediately to have direct impact on security across multiple domains.

Academia

1. *Partnerships and Joint Course Offerings Between Science/Engineering Departments and Policy/National Security Programs*: Building this kind of cross-department learning into program requirements will begin to develop the skills needed to create the type of professional being sought by public and private sectors.
2. *Consulting Practicums*: In-class learning should be paired with experience-based learning that mirrors the real world. Partnerships between academic institutions and private companies will give students experience operating in a private sector environment and responding to challenges that impact their mission. This experience can be carried forward into any future job as added value.
3. *Professional Upskilling Offerings*: Starting with degree-seeking programs will not be sufficient as the current workforce needs to be trained today. A robust offering of professional development courses will give established professionals the ability to bring new skills to their already deep experience providing immediate impact and value to their organizations.

Private Industry

1. *Fellowship Programs with Governments*: Industry and government need to speak the same language and opportunities to bring government professionals into private firms and private professionals into government offices on a temporary basis would create immediate value.
2. *Integration of Emerging Technology Talent with Cybersecurity Teams*: Focusing only on cybersecurity is only fighting half the battle. Emerging technology professionals can focus on the goals of the cyber intrusion to help vector defenses and speed up recovery.
3. *Funding for STEM Professional Development*: Private companies should increase professional development funding for STEM fields to give all employees a better view into the critical context all firms operate inside.

Practical Application

Cyber programs in academia abound because they've had 30 years to mature. Emerging technology programs are just beginning as top universities respond to the demands from industry and governments. Creating unique student experiences that prepare them for practical realities must reflect the environment in which they will operate. Homeland security professionals are securing a homeland that includes the most valuable strategic assets our country possesses, our innovation ecosystem and its products. Those assets are also targets meaning that analysts,

officers, and agents throughout the homeland security enterprise will need to be able to recognize the reasons behind cyber intrusions, not simply that one has occurred. Mitigating cyber events remains important but why the event occurred at all is key for practitioners so they can prevent the next one. Critical infrastructure will continue to be both enhanced and threatened by emerging technologies as new capabilities and use cases emerge. The security of the homeland does not hinge on the development of any specific technology but of the people who are managing risk and evaluating opportunities. Those people must be prepared and have an academic partner who will continue to provide them with updated content throughout their professional journeys.

Remaining geopolitically competitive and maintaining our national security means having and securing a robust innovation ecosystem. That ecosystem is inside the homeland and contains private companies. Those companies are targets of well-resourced cyber actors who seek their valuable intellectual property, and this dynamic will define this era. Emerging technology as a profession is in its earliest stages of life, but the requirements are present today. Academic institutions have the opportunity to create a strong program to meet student needs throughout their career lifecycle keeping them relevant and valuable to organizations. Further, academic institutions can avoid a situation mirroring the cyber field where degrees and certificates are no longer strictly necessary for employment. The inflection point is now.

Appendix A: Sample Cyber Job Descriptions

Key Role:

Perform advanced analysis of adversary tradecraft, malicious code, and capabilities. Provide intelligence analysis of cyber threats and develop briefings and reports to distribute and aid in information sharing and protection efforts among senior government members and Combatant Commands. Develop and maintain subject matter expertise of Advanced Persistent Threats and assist with Incident Response efforts. Perform advanced research into threat actor and adversary capabilities, and develop custom threat intelligence reports to assist ongoing mission efforts.

Basic Qualifications:

- Experience with extensive military and cyber threat operations
- Ability to work in a high paced and dynamic work environment
- TS/SCI clearance
- HS diploma or GED and 8 years of experience in IT and cyber threat information, or Associate's degree and 6 years of experience in IT and cyber threat information

Additional Qualifications:

- Experience in the Joint Staff or other U.S. Military Staff
- Experience with Microsoft Office products
- Knowledge of JCIDS
- CISSP, GREM, GCIH, or GCIA Certification
- Completion of DAU training

Clearance:

Applicants selected will be subject to a security investigation and may need to meet eligibility requirements for access to classified information; TS/SCI clearance is required.

Compensation

At Booz Allen, we celebrate your contributions, provide you with opportunities and choices, and support your total well-being. Our offerings include health, life, disability, financial, and retirement benefits, as well as paid leave, professional development, tuition assistance, work-life programs, and dependent care. Our recognition awards program acknowledges employees for exceptional performance and superior demonstration of our values. Full-time and part-time employees working at least 20 hours a week on a regular basis are eligible to participate in Booz Allen's benefit programs. Individuals that do not meet the threshold are only eligible for select offerings, not inclusive of health benefits. We encourage you to learn more about our total benefits by visiting the Resource page on our Careers site and reviewing Our Employee Benefits page.
Salary at Booz Allen is determined by various factors, including but not limited to location, the individual's particular combination of education, knowledge, skills, competencies, and experience, as well as contract-specific affordability and organizational requirements. The

projected compensation range for this position is $81,800.00 to $186,000.00 (annualized USD). The estimate displayed represents the typical salary range for this position and is just one component of Booz Allen's total compensation package for employees.

Work Model
Our people-first culture prioritizes the benefits of flexibility and collaboration, whether that happens in person or remotely.

- If this position is listed as remote or hybrid, you'll periodically work from a Booz Allen or client site facility.
- If this position is listed as onsite, you'll work with colleagues and clients in person, as needed for the specific role.

EEO Commitment

We're an equal employment opportunity/affirmative action employer that empowers our people to fearlessly drive change – no matter their race, color, ethnicity, religion, sex (including pregnancy, childbirth, lactation, or related medical conditions), national origin, ancestry, age, marital status, sexual orientation, gender identity and expression, disability, veteran status, military or uniformed service member status, genetic information, or any other status protected by applicable federal, state, local, or international law.

Responsibilities:
Peraton is seeking a Threat Hunting Analyst to join our team of qualified and diverse individuals. The qualified applicant will become part of Department of State (DOS) Consular Affairs Enterprise Infrastructure Operations (CAEIO) Program, for the Bureau of Consular Affairs (CA). This initiative is to provide IT Operations and Maintenance to modernize the legacy networks, applications, and databases supporting CA services globally.

Day to Day Work Responsibilities:

- Conducts research and data correlation using a variety of enterprise data sources with specific emphasis on network operations and cyber warfare tactics, techniques, and procedures.
- Analyzes network events to determine the impact on current operations and conduct research to determine adversary capability and intent.
- Analyzes identified malicious network and system log activity to determine weaknesses exploited, exploitation methods, effects on systems and information.
- Collects and analyzes network device integrity data for signs of tampering or compromise.
- Prepares assessments and cyber threat profiles of current events based on the sophisticated collection, research, and analysis of information.
- Conducts data analysis in support of directed assessments, anomaly investigations, long term trending and system check out.
- Develops and maintains analytical procedures to meet changing requirements and customer inquiries.

- Serves as the cyber technical liaison to stakeholders, explaining investigation details.
- Tracks and documents incident response activities and provides updates to leadership through executive summaries and in-depth technical reports.
- Create, discuss and explain Cyber investigative documentation.
- Resolve highly complex malware and intrusion issues using computer host analysis, forensics, and reverse engineering.
- Characterize and analyze network traffic, identify anomalous activity / potential threats, and analyze anomalies in network traffic using metadata.

Qualifications:

Basic Qualifications:

- US Citizenship required and an active **TOP SECRET** clearance.
- BS degree and 12 to 15 years', experience or MS degree with 10 to 13 years', experience or a high school diploma/equivalent with minimum 16 years', experience.
- Possess CISSP or similar cybersecurity certification.
- 8+ years of directly relevant experience in cyber forensic and network investigations using leading edge technologies and industry standard forensic tools.
- Experience with reconstructing a malicious attack or activity.
- In depth knowledge and experience of identifying different classes and characterization of attacks and attack stages.

Preferred Qualifications:

- Knowledge of cybersecurity frameworks and standards
- Ability to track incidents using MITRE ATT&CK and Cyber Kill Chain methodology.
- Knowledge of cloud security
- Knowledge of current IT security best practices
- Knowledge of system administration, networking, and operating system hardening techniques
- Mixed operating systems experience: (Linux, Windows)
- Scripting/coding experience

Shift/Hours: 1st Shift - Monday through Friday

Peraton Overview:
Peraton drives missions of consequence spanning the globe and extending to the farthest reaches of the galaxy. As the world's leading mission capability integrator and transformative enterprise IT provider, we deliver trusted and highly differentiated national security solutions and technologies that keep people safe and secure. Peraton serves as a valued partner to essential government agencies across the intelligence, space, cyber, defense, civilian, health, and state and local markets. Every day, our employees do the can't be done, solving the most daunting challenges facing our customers.
Target Salary Range: $146,000 - $234,000. This represents the typical salary range for this position based on experience and other factors. EEO Tagline (Text Only): An Equal Opportunity Employer including Disability/Veteran.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security Sam Houston State University

Reese, N. (2023) Convergence of Mission and Moment: Imagining the Emerging Technology Analyst. (Report No. IHS/CR-2023-1025). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/JXWRF