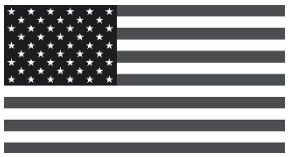
MITRE



MITRE TECHNICAL REPORT

Cyber Strategy Development & Implementation Framework
(version 4.0)

Cyber Capacity Building

Sponsor: U.S. Department of State
Dept. No.: Office of the Coordinator for Cyber Issues (S/CCI)

Contract: **SAQMMA17C0341**
SAQMMA17C0346

McLean, VA

Authors:
Stacie Y. Duhaney
Richard B. Harris
Johanna G. Vazzana
Cynthia A. Wright

September 2020

Approved for Public Release, Case Number 20-2683

Abstract

The Cyber Strategy and Implementation Framework draws from the best practices of more than 18 US, International, and Industry models. It uses a combination of design thinking activities, threat/opportunity/resources contextualization, and a lens of eight key cyber capacity areas in a four-phase strategy approach to assessing cyber needs and threats, developing risk-informed strategic goals, identifying and prioritizing supporting objectives and initiatives, and implementing them in a multi-stakeholder environment. This fourth version of the Framework draws from lessons learned during its application in more than a dozen countries and three US government agencies. It slightly modifies the Eight Key Cyber Capacity Areas to allow for differentiation between civil law/regulation and policy/standards, and between operational resiliency and incident response. It also elevates Strategic Foundations to its own pre-requisite set of activities and capabilities, and acknowledges that Partnerships is not a stand-alone capacity area, but rather one that informs every other capacity area, as well as Strategic Foundations (particularly Stakeholder Involvement). This edition also addresses organizational level strategy as well as national level strategy development requirements. Finally, it adds the Cyber Workforce Development Framework and other products to its library of tools and approaches for cyber strategy development and capacity building teams.

 Approved for Public Release, Case Number 20-2683

This page intentionally left blank.

Approved for Public Release, Case Number 20-2683

Table of Contents

List of Figures

This page intentionally left blank.

Approved for Public Release, Case Number 20-2683

1 Introduction

Human, societal, and commercial dependence on information and information communication technologies (ICT) is increasing across the globe. These technologies support key business and mission applications, enable the extension of essential services, support more efficient oversight of critical processes, provide access to global communities and knowledge, and deliver data used in applications, analyses, and processes essential to modern economies. At the same time, by connecting previously separate systems and allowing unmediated access between individuals and entities, they introduce or increase the risk of compromise, manipulation, denial of services, extortion, fraud, and other crimes, and even the destruction of systems and data. To take advantage of the opportunities and mitigate the risks of cyber-related technologies, countries and organizations must actively integrate their technological capacity building with their broader strategic goals, building in security and privacy protections, as well as effective and transparent governance. Because **cyber capacity is a means to many ends, rather than an end in itself**, it is important to develop a cyber strategy that focuses on articulating and implementing a vision for an ICT environment that furthers strategic objectives; is reliable, interoperable and secure; that recognizes the need for coordinated efforts among multiple stakeholders to achieve goals; and that functions as an authoritative mandate that enables action.

The purpose of a national or agency cyber strategy is to provide high-level guidance on cyber-related capacity development by articulating and prioritizing objectives, outlining supporting policy and structural mechanisms, establishing roles and responsibilities, allocating resources, and identifying measures of effectiveness. **Published cyber strategies educate and inspire internal audiences**, explaining why and how the country or organization plans to leverage technology to achieve business, political, economic, social, and security aspirations. By communicating intentions and priorities, cyber strategies can also **help inform strategic partners** and **deter potential or known adversaries** and criminals. Conversely, the lack of an explicit strategy can raise questions as to the openness, efficacy, and legitimacy of national or organizational policies and activities in cyberspace.

Because political and administrative systems differ, some countries or organizations signal their priorities not through a single strategy document, but through other instruments such as legislation, published policy, resourcing decisions, and development plans that reflect their evolving capacity and needs. **More important than the process or structure of the mechanism is its deliberate and determined implementation—issuing a strategy does not end but rather starts the real work.** Strategy is a continuously on-going process of assessment, development, and implementation, followed by reflection and re-assessment. Whatever approach is followed, a cyber strategy must be tailored and periodically re-adjusted to match operational, political, economic, financial, and technological needs and aspirations, within an ever-evolving risk/opportunity context.

The U.S. Government has a strong interest in helping agencies and governments develop, commit to, and implement responsible, comprehensive, forward-looking cyber strategies and policies that increase their technological capacity, secure critical functions and information, and help achieve national goals while fostering a strong international security environment and associated norms and standards.[1]

1.1 Why Use This Cyber Strategy Development & Implementation Framework?

Many U.S., international, and industry organizations and groups have published guides for national cyber strategy development. Among those are the Cooperative Cyber Defense Center of Excellence (CCD COE), the Commonwealth Telecommunications Organisation (CTO), the European Union Agency for Network and Information Security (ENISA), the International Telecommunication Union (ITU) and other elements of the United Nations, Microsoft, the Oxford Global Cyber Security Capacity Centre, and the Organisation for Economic Co-operation and Development (OECD). New tools and guides appear regularly, and additional insights can be found in documents pertaining to Internet governance and security, discussions on specific emerging technologies (such as Cloud Services) and their political, economic, and security implications, national and international debates about data sovereignty and roles and responsibilities appropriate to securing the "global commons" of cyberspace, guidance for Chief Digital Officers, National Cybersecurity Coordinators/Advisors, and governance institutions, and international conventions regarding data privacy, cybercrime, and cyber war.

The CSDI model identifies and incorporates the strengths of many global approaches.

The *Cyber Strategy Development and Implementation (CSDI) Framework* (Framework for short) was developed to integrate the strengths of these approaches into a single comprehensive model. It is a phased approach that applies a strategic mindset to the task of building cyber capacity at both national and organizational levels using a set of key capacity areas drawn from global best practices. **This Framework is designed to inform cyber strategy development and implementation efforts within each nation or organization's particular risk/opportunity landscape, and according to its unique needs and aspirations.** It offers guidance and tools for thinking strategically about cyberspace and creating an optimal environment for leveraging ICT to reach strategic goals. In addition to taking an intuitive, multi-stakeholder approach to prioritizing strategic objectives and supporting initiatives, it focuses on the preliminary and enabling activities essential to cyber strategy development and implementation—such as threat/opportunity context analysis, risk-informed goal prioritization, stakeholder involvement, creating and leveraging partnerships, and establishing supporting organizational structures. It provides suggestions for addressing these preparatory elements; offers tools and approaches for systematically assessing current capabilities within the contexts of operational, political, security, social, and economic goals; and provides methods for creating implementation roadmaps toward capacity development in prioritized areas. Among these tools are a variety of assessments, as well as materials on planning, governance, standards and

[1] For the US international cyber policy see *National Cyber Strategy of the United States* (Washington D.C.: The White House, 2018).

policies, workforce development, organizational change and strategic communications, and guidance for improving resilience through partnerships, playbooks and exercises, and the establishment of world-class cybersecurity operations centers.

Throughout, this Framework acknowledges the unique contexts and needs experienced by different countries and organizations while recognizing the common values of determined leadership, frank assessment and communication, effective prioritization of efforts within available resource constraints, and the inputs of various stakeholders as the key qualitative factors in a successful strategy process. These values and approaches can be applied at the organizational, national, or regional level, bilaterally or multilaterally, and in any phase of the strategic planning cycle to build cyber capacity that supports the specific needs of individual organizations, organizations, geographic regions, or communities of interest.

1.2 Methodology

1.2.1 Assumptions

The CSDI Framework was developed based on the following assumptions:

- There is no one-size-fits-all model for cyber strategies or capacity building.[2] Each nation's or organization's goals and approaches should reflect its needs, resources, and particular risk environment.
- The fundamental elements of assessing and planning for cyber capacity building are universally applicable. In addition to the four phases typical of strategic planning models, the CSDI's eight capacity elements and their pre-requisites are drawn from international best practices in cyber strategy development.
- Cyber capacity cannot be effectively described using a static maturity model or objective scale. Though the key capacity areas and capability ranges within those areas can be described, desired end-states for a particular entity should be determined solely by their risk-informed goals, and priorities should be based on compared to their existing capacity needs to those goals. In other words, a particular capacity level in a given area may be insufficient

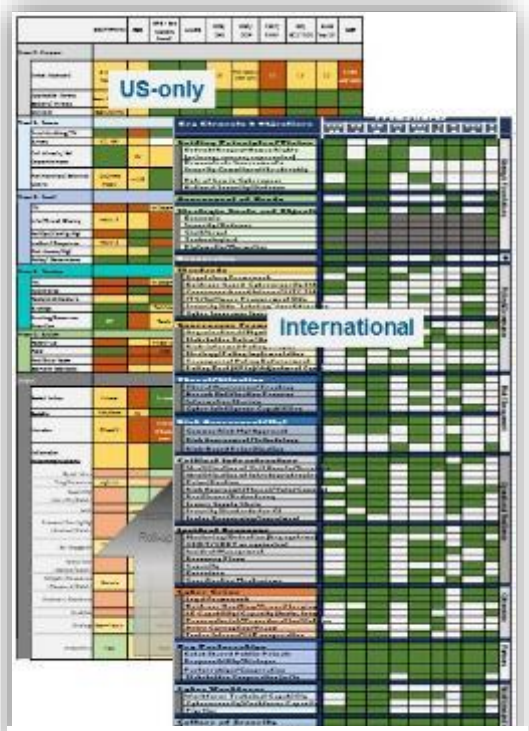


Figure 1: MITRE's mapping of U.S., International, and Industry Cyber Strategy models is the basis of its 8 Cyber Capacity Areas

[2] Throughout this paper, "cyber capacity-building" is often used nearly interchangeably with "cyber strategy" because cyber strategies and related approaches are typically based on a desire to increase capability and/or capacity in particular functional areas that will support specific, higher level goals such as economic growth, security, etc.

for some entities, but adequate for others with different risk landscapes and objectives.

In developing this Framework, MITRE analysts reviewed numerous respected cyber strategy and capacity assessment tools (others have been added since) to gain a sense of what indicators are considered desirable by a variety of experts, each with different perspectives (see Appendices A and B). During comparative analysis, key subjects addressed in each instrument were evaluated (Figure 1) to inductively identify 1) those elements that are common across many respected assessment and strategy guides—the "must haves," and 2) elements that are not commonly addressed but were identified in one or more tools and have relevance to national cyber strategy development, such as resourcing strategies, or market incentives. Finally, these subject areas were then grouped by theme, with the individual elements retained as assessment criteria.

1.2.2 Four-Phase Strategy Approach

The Framework was developed to be useful across a wide range of circumstances using a four-phase approach. Engagement can begin in any phase.

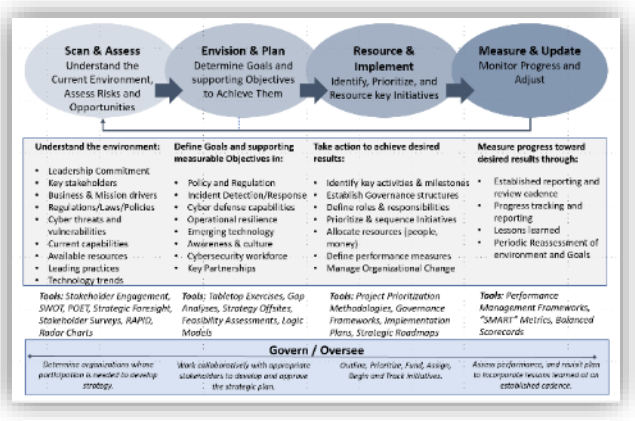


Figure 2: The 4-Phase Strategy Process

Phase One - Scan and Assess: Activities in this phase provide important political, economic, technological, and social background on a nation or region in the context of cyber capacity building to inform engagement activities. Key factors such as existing laws, policies, threats, and opportunities, as well as current cyber capacity in the eight key areas—particularly the Strategic Foundations—are identified. While the CSDI framework includes an assessment specifically designed for it, other assessment tools such as POET (Politics [or Policy], Operations, Economics, Technology) or other cyber-specific instruments can also be adapted for the environmental scan.

Phase Two – Envision and Plan: Cyber strategy development is best accomplished through an iterative series of engagements involving senior managers and technical stakeholders from across the stakeholder ecosystem. It is often helpful if the initial activities are facilitated by outside experts (whether MITRE, or other advisory team) who can help a group with diverse and often competing interests work together to identify and pursue common goals that may or may not directly benefit them individually. Initially, these engagements are often not focused on strategy development per se, but rather on developing a **common situational awareness and vision of the future**, weighing risks and opportunities, identifying and prioritizing potential capacity building goals, ideating and evaluating solutions, and building support through strategic communications.

The Design Thinking process is an innovation model that leverages diverse groups of stakeholders and iterative cycles of ideation and refinement to arrive at consensus solutions to complex problems.

Approved for Public Release Case #20-2683.

Described in this way, cyber strategy development resembles the classic description of Design Thinking, employed by the Stanford D-School, IDEO, Harvard, and numerous innovation facilitators in the private sector around the globe. The Design Thinking process is an innovation

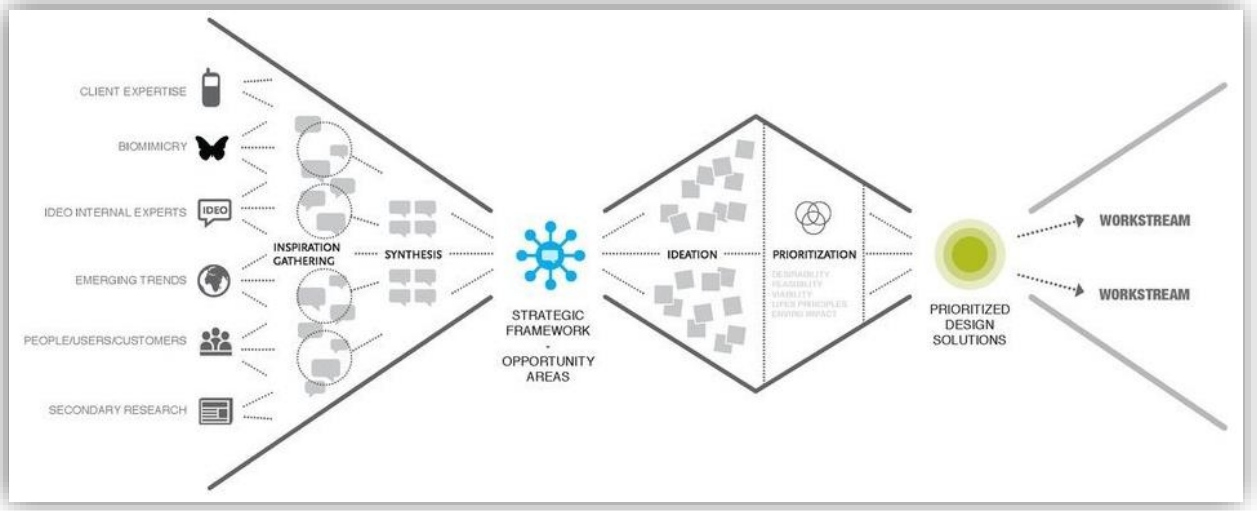


Figure 3: The Design Thinking Ideation Process

model that leverages highly diverse groups of stakeholders and subject matter experts in iterative cycles of ideation, refinement, and evaluation to arrive at consensus approaches to identifying and implementing solutions to complex problems. One visual representation of this process (IDEO's) is shown in Figure 3.

In this phase, strategy teams develop mission-oriented ("Big Picture") goals based on the findings from Phase 1, and then identify how cyber/ICT investments can support those goals. The CSDI framework uses a capacity gap assessment and risk management approach to identify and prioritize focus areas that address the most pressing threats and/or opportunities and develop appropriate initiatives with objectives with actionable supporting initiatives. The gap analysis is usually depicted in a "radar chart" like the one at right, where the orange line shows goals, and the blue shows current capacity (see "eight key capacity areas" below). Because no nation or organization has unlimited resources, one of the key functions of this kind of chart is to **help stakeholders *prioritize***—to determine actionable strategic objectives that focus specifically on a threat or opportunity gap they want to address. Combined with a realistic threat assessment from Phase 1, this approach helps stakeholders prioritize actions within their available resources by applying a risk management approach—it helps stakeholders visualize their greatest needs while considering what threats may also require attention. The key aspect of this approach, which differentiates it from others in common use, is that it uses the nation or organization's own desired end-state, rather than some ideal "maturity level" to help illustrate gaps, which are grouped into

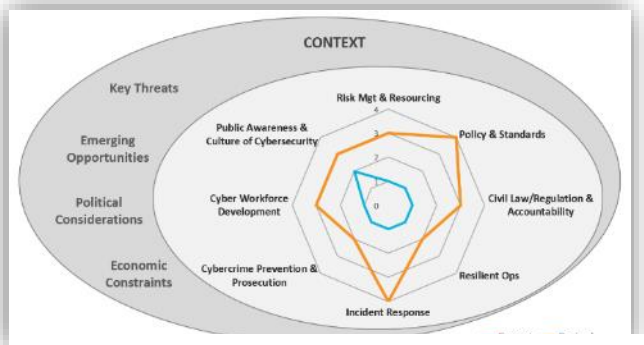


Figure 4: Cyber capacity gap analysis

the eight key capacity areas to facilitate a strategic perspective. This helps ensure that, for example, a country that needs to focus on resilience to national disasters is not distracted by trying to increase their "maturity" in civil law or incident response to APT threats. In short, countries or organizations can use this chart to help **simplify the strategic landscape in a way that facilitates developing manageable and meaningful strategic goals and objectives.**

A key aspect of this approach is that it uses the organization's own desired end-state, rather than some ideal "maturity" level to illustrate and prioritize strategic capacity gaps.

Once these gaps are identified, the team applies a risk/benefit analysis based on the contextual threat/opportunity assessment from Phase 1 to agree on 3-5 strategic Goals (more than five strategic goals is likely to spread implementation resources too thin). Ideally, this activity is conducted over a 2-3 day engagement at the senior leadership level in order to ensure broad commitment to a set of agreed-upon strategic goals from which a guiding Strategy can be drafted. These Goals represent the nation's or organization's desired "ends" *at the completion of the current strategy cycle.* In cases where a multi-day engagement is more than what is desired, the tools associated with this phase can be used separately on a smaller scale such as in stand-alone workshops. In either case, it is important that decision-makers from as broad an array as possible of stakeholder organizations—not just ICT entities—participate, in order to gain the "buy-in" that will be essential for implementation and the prioritized allocation of resources.

Once the Strategic Goals are articulated, the team (typically comprising functional experts a level or two below senior leadership) considers and selects supporting Objectives (steps or "ways" to achieve the Goals), which will in turn be implemented through specific, actionable Initiatives (the "how" or "means" of the strategy). For example, if one goal involves transitioning to an e-services environment, a supporting objective might be enabling seamless information sharing across applications. Two enabling initiatives might be establishing a data standardization policy, and refreshing some technology to improve interoperability. A second Objective might address the creation of a tech-savvy public or customer base, and a supporting initiative might be the development of an external messaging campaign.

In ideating and selecting Initiatives, the CSDI model favors the design thinking approach referenced above, which includes many tools (Figure 5) for brainstorming initiatives, converging and modifying them, prioritizing and down-selecting to a manageable number, and then mapping stakeholders and processes for implementation. Other approaches to this step include various logic models, such as COPIS (Customer, Output, Process, Inputs, Supplier), Services Model Canvas, or similar tools that rely more on process mapping. Which approach a team uses

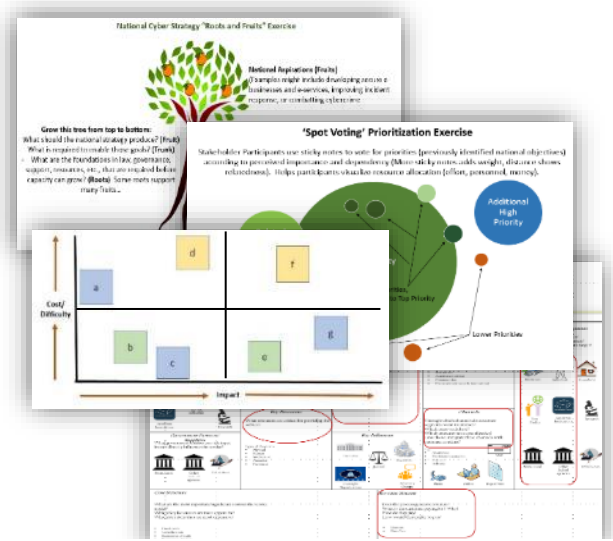


Figure 5: Design Thinking Strategy Tools

often reflects the breadth and intent of the strategy—a broad national or organizational mission-focused strategy may use the design thinking approach, while a narrower strategy focused on optimizing a particular set of functions may benefit from a logic model approach.

At the end of this phase, the strategy should be fairly well articulated, outlining at least the framing context, and the resulting Goals, Objectives (steps to achieving the goals), and Initiatives (specific programs or activities that comprise the objectives). It likely also identifies the top-level offices that will be instrumental in execution, and the method or source of resource allocations. Some strategies will also include a more detailed implementation plan (see Phase 3), but this is often captured in a separate document so that specific timelines and metrics can be adjusted as changing circumstances may warrant without the need to re-coordinate the strategy itself.

Phase Three – Resource and Implement: In this phase, teams identify the major activities that will be required for implementation, detail stakeholder roles and responsibilities, sequence events, allocate human and fiscal resources, assign key functions, and establish milestones and metrics. This is the most complex and time-consuming phase, and the one most subject to change in response to changing circumstances over the course of the strategy cycle. For that reason, it is often achieved through a set of related implementation plans or roadmaps that are executed by different stakeholder subsets. Even in this case, however, central oversight and accountability are key to making progress—particularly in the face of unexpected challenges or changes in priorities or resources.

It is important to manage expectations with regard to the time and effort required to move from a high-level articulation of strategy to fleshing out the details required to make that strategy a reality.

It is important to manage expectations with regard to the time and effort required to move from a high-level articulation of strategy to fleshing out the details required to make that strategy a reality. Though settling on the level of direction and detail described in Phase 2 can often be accomplished in a few weeks, Phase 3 will take most organizations much longer—this is a natural

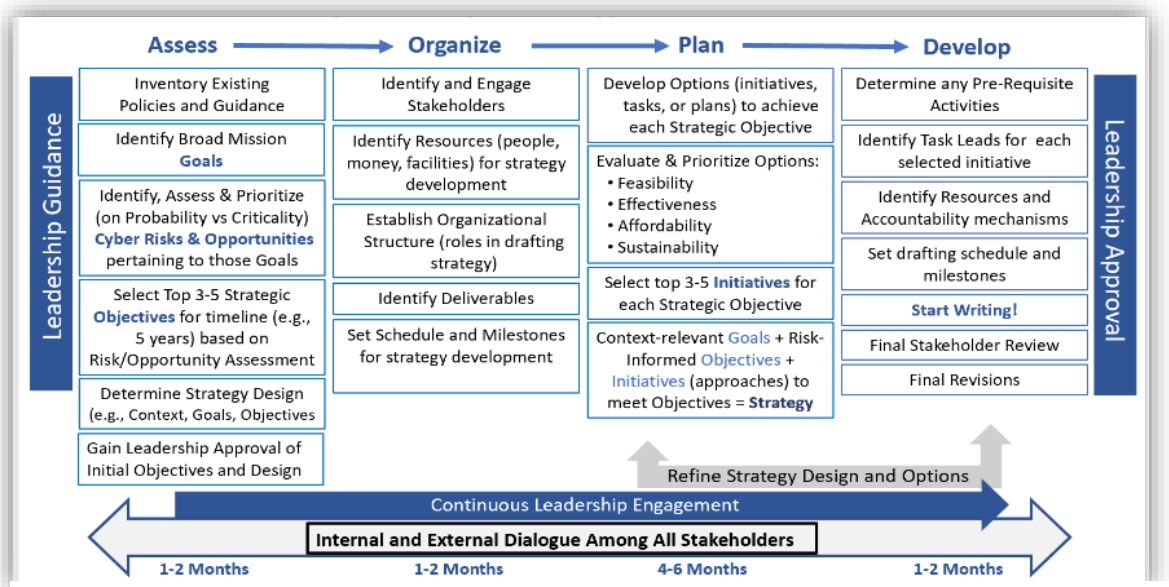


Figure 6: Overview of the Strategy Development Process

manifestation of the many factors that must be considered and adjudicated in actually determining how to implement a strategy—the money and people required, the governance mechanisms that must be established of modified, the details of program design, sourcing, and execution that will affect timelines and cost. The detailed implementation plan that emerges from this phase is complex and sometimes technical, different portions of it will have more or less relevance to different stakeholders, and various initiatives will require shorter or longer timelines, with varying degrees of complexity. For that reason, this phase is usually conducted by smaller working groups, and the implementation plan—which may be a single document or comprise one document per initiative—is often developed, published, and maintained separately from the overarching strategy so that individual portions of it can be adjusted as needed in response to changes in circumstances. The graphic above depicts a notional timeline for Phases 1-3 of cyber strategy development (it does not include Phase 4).

Phase Four – Measure & Update: Strategy is an ongoing, iterative process. Strategic initiatives are rarely discrete activities that can be completed and forgotten—they require "lifestyle changes" that involve conscious follow-up and measurement, and continued investment of time and resources. As the strategic environment evolves, and nations or organizations increase their capacity, strategic goals and objectives will change. The strategy process is therefore continuous and iterative, typically comprising 2-5 years per cycle. Revalidation, however, should be ongoing throughout. In this phase, strategy teams revalidate and adjust strategic approaches in light of changing circumstances and/or activities that have stalled or proven ineffective and take stock of the progress toward strategic objectives using defined metrics or other measures. These appraisals feed back into the next strategy cycle, starting with a re-examination of the environment. This phase will begin at different times for different implementation plans, as some initiatives will be completed more quickly than others. This phase also offers an ideal opportunity to communicate with stakeholders about progress and challenges, and to identify and organizational change issues that may need to be addressed.

2 CSDI Framework Overview

The CSDI framework uses the phased approach described above to help nations and organizations navigate their cyber strategy needs, focusing the assessment and planning phases through the lens of eight key capacity areas, as well as some "pre-requisite" elements that represent the building blocks or "strategic foundations" of cyber capacity-building. The Eight Key Capacity Areas and their Foundations are described in detail below.

2.1 Strategic Foundations

The following elements are considered pre-requisites to effective strategy development—they are not capacity areas per se, but represent the **"strategic foundations"** of cyber capacity-building.

- **Context/Threat Awareness**: an understanding of how cyber and ICT shape the strategic environment, and the specific threats that exist or can be anticipated with regard to critical systems, services, and data.
- **Connectivity/Access**: a minimum level of internet access by constituents and strategic partners is typically important in both informing and enabling cyber-related goals. Where connectivity/access is insufficient, the initial cyber strategy may be an ICT for

Development effort, focused on expanding that access in a cost-effective and secure manner.

- **Leadership Commitmen**t: the public and private recognition by national/organizational leadership of the essential role these technologies and capacities play in executing and protecting important functions, and their commitment to investing in them.
- **Mission-focused Goals**: goals that reflect the nation's or organization's long-term objectives in areas such as mission capability, economic prosperity, political legitimacy, functional resilience, situational awareness, partnerships, competitive advantage, health and education, service delivery, etc., determine how and to what degree ICT and related capacities are essential to progress. These mission-focused goals are the "what" of strategy—the specific cyber-related initiatives are the "how."
- **Stakeholder Involvement**: recognition of the indispensable role played by an ecosystem of stakeholders in identifying and achieving strategic cyber-related goals. Stakeholders typically include government, industry, civic, legislative, and regulatory entities, as well as suppliers, operators, and citizens/customers.

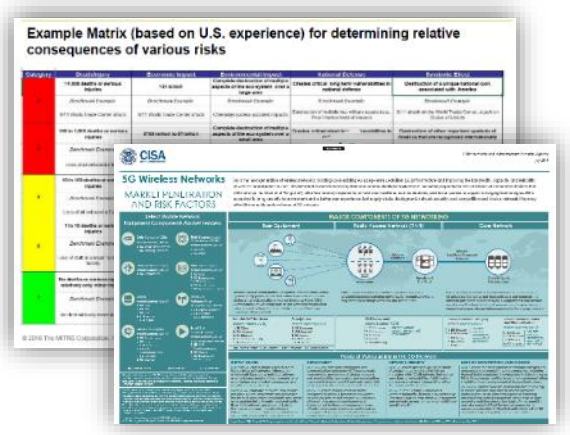
2.2 The Eight Key Cyber Capacity Areas

Once these strategic foundations are in place, or at least substantially in work, strategists can begin to focus on priorities in the **Eight Key Cyber Capacity Areas.** These fall into three categories: governance, operational, and enabling activities (Figure 7). Each represents an important element in a nation or organization's ability to achieve their cyber-related objectives. They are described in detail below.

Figure 7: The Eight Key Cyber Capacity Areas

2.2.1 Risk Management & Resourcing

Prioritization is almost invariably one of the most difficult aspects of both developing and implementing strategy. In a 1996 *Harvard Business Review* article, Michael Potter summed this up, noting "the essence of strategy is choosing what *not* to do." Because cyberspace crosses and connects so many functional areas, stakeholder groups, and technologies, the potential opportunity space is immense—organizations at all levels find themselves faced with a plethora of possible investments ranging from the mundane and nearly invisible (but essential), such as software licenses, to the cutting edge and inspirational, such as artificial intelligence and 5G.



A deliberate Cyber Risk Management approach that weighs various opportunities and threats in terms of their likelihood and potential consequences or return on investment within the given operational context is essential to creating both focus and stakeholder buy-in. A Risk Management approach provides stakeholders with the objective comparisons that help narrow the list of potential strategic initiatives to those that will have the greatest impact on their strategic capacity and security.

By involving stakeholders in the risk determination and prioritization process, teams develop a common understanding of, and consensus on, priorities.

Once they have participated in this process, they are more likely not only to support, but to defend, the next critical step: resource allocation. Generally speaking, no organization has the resources it needs to do everything it wants. Decisions must be made on where to allocate limited funds and personnel. While many organizations attempt to appease all stakeholders by allocating them some proportional amount of resources to pursue their preferred initiatives, this approach typically results in no office having enough resources to effectively achieve their objectives. Instead, the larger organization is left with many partially completed efforts, none of which meaningfully advances its strategic objectives. By involving stakeholders in the risk determination and comparison process, teams can develop a common understanding of, and consensus on, priorities—even where the priorities that emerge do not reflect their individual "wish lists"—which in turn translates to an understanding of where it is most important to focus their limited resources. While some desired initiatives will be tabled in this process, the highest priorities stand a much greater chance of being fully executed, raising overall capacity and increasing the likelihood that other priorities will rise to the top and be completed in the next strategy cycle.

2.2.2 Civil Law, Regulation, & Accountability

Taking full advantage of the opportunities cyberspace offers while mitigating risks and assuring privacy, transparency, and accountability, requires strong legal frameworks that should be

addressed as a component of cyber capacity-building efforts. In some cases, they will have to expand or limit their preferred approaches to comply with law and regulation. In others they will need to establish these regulations in order to assure stakeholders of the security and appropriate use of their key systems and data. This capacity area includes basic cybersecurity-related legislation and regulation, such as data protection and privacy laws, civil definitions of protected systems and prohibited activities—such as are delineated in the international Budapest Convention on Cybercrime—data breach notification and liability protections, standards pertaining to the protection of critical infrastructure and key resources or services, and the establishment and governance of Cyber Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs). It also includes government organization around cyber initiatives and policy development, cyber-related authorities for such activities as law enforcement and defense, oversight/compliance mechanisms, technology acquisition rules and processes, the ability to request and earmark resources, and other centrally determined activities. In some countries, it may address seemingly peripheral issues, like compensation for government workers or primary school curriculum standards, that will prove to be important to overall cyber capacity.

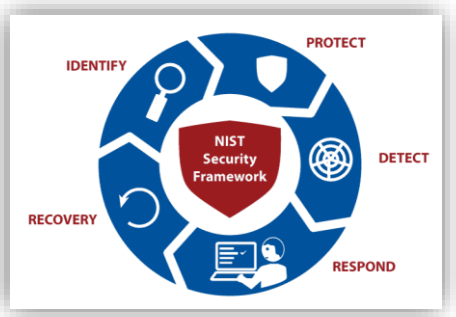
Entities seeking to increase capacity in this area often focus on drafting legislation that conforms to international best practices and standards. Another key focus area is in defining roles, responsibilities, and authorities. Even within organizations, stovepipes between legally mandated functions can create interoperability and/or security issues—at the national level, gaps, overlaps, and ambiguities in roles and responsibilities can hinder information sharing, create distrust among agencies, perpetuate inequitable and inefficient resource distribution and standards compliance, complicate incident response, and slow post-incident recovery efforts. Therefore, it is important that roles and responsibilities for policy development, resourcing, standards determination and compliance/audits, data sharing and protection, law enforcement, intelligence/surveillance, defense, incident response, monitoring, and interagency coordination be carefully considered and formally addressed. It is often not possible to completely deconflict legal authorities, as many activities in cyberspace overlap, so establishing formal processes for adjudicating issues where legal mandates overlap (for instance, between law enforcement and intelligence agencies) is important.

At the national level, one of the most transformative strategic activities in this capacity area may be the formal (legislated) establishment and empowerment of a national cyber coordinator. In many countries, this can help speed the government's digital transformation by eliminating the need for lengthy legislative deliberation processes in favor of a well-qualified and neutral expert with oversight over fundamentals like cybersecurity technical standards, reporting procedures, and data protection. This position may also oversee resourcing and contracting processes related to technology purchases to ensure interoperability, security, and supply chain integrity, and act as a central point of contact for internal stakeholders and outside partners, strategic messaging related to cyberspace or ICT, and interagency policy coordination. At the organizational level, an analogous position might be a Chief Information Officer (CIO), Chief Information Security Officer (CISO), or Chief Data (or Digital) Officer (CDO)—such an office should similarly be

empowered to make resourcing recommendations, oversee ICT-related contracts and purchases, develop overarching cybersecurity standards and oversee compliance.

2.2.3 Policy & Standards

This capacity area addresses the specific mechanisms through which a cyber strategy is articulated, implemented, and enforced. At the least, it is likely to include the selection, adoption, and compliance oversight of cybersecurity and engineering technical standards for particular systems or classes of system (such as sector-specific critical infrastructure or essential e-services). This capacity area is separate from Law and Regulation because it is intended to address the capacity to make and enforce policy below the national level.



Because many countries do not have this intermediate capacity, but rely exclusively on a combination of law and high-level Presidential or Ministerial Directives, this may be a focus area for many national governments. Having a cyber policy-making institutional capacity in organizations responsible for overseeing aspects of cyber capacity is important because cyber threats, technologies, and standards changes more often, and at a finer level of detail, than is typically feasible to address legislatively. Moreover, it requires a significant level of technical subject matter expertise among designated staff that is often not extant in legislative bodies. It can be difficult to establish a policy mechanism where none has previously existed, particularly if there are prohibitions based on fear of corruption or subversion of democratic processes. For this reason, it is important when building capacity in this area to establish safeguards and controls such as transparency requirements, appeals mechanisms, and whistleblower protections. It may also be possible to shape policy-making authorities by tying them to international best practices and standards.

One significant consideration in this area, for both nations and organizations, is the selection and implementation of cybersecurity standards. It is important that the application of such standards be uniform, so that there is no perception that they are enforced unevenly or used to manipulate or punish. It is also important that the selection of standards be based on international best practices, and that applying these standards takes into account both the expense and learning curve that may be involved in the transition. For example, simply requiring that all systems and software in key functions be licensed and vendor-supported with updates and patching may necessitate a massive overhaul in organizations' systems that they do not have the internal resources—either fiscal or human—to implement over a short timeframe. Both governments and organizations can help facilitate the institution of security and interoperability standards by centrally budgeting for incremental (e.g., one office or function at a time) implementation, and then providing assistance through CSIRTs or CERTs and training initiatives (see Workforce Development, below). Policy that establishes new standards should also address change management—not only requirements for patching and updates, but also oversight over new purchases or enterprise changes that might affect operations, security, or long-term sustainment.

Finally, policy typically addresses user behavior on certain defined (such as government, critical infrastructure, or essential operational systems), to include what kinds of internet connections are

allowed, identity and access management provisions such as password requirements, data protection expectations, what websites may be visited or applications loaded, what devices can be connected and the procedures that govern that approval, what kinds of files may be accessed on key systems and transmitted/processed outside of those systems, and any scanning or malware protections that may be required. Capacity in this area also includes the ability to assess and enforce compliance. Accordingly, policy makers may have oversight over cybersecurity and information security user training, traffic monitoring on designated systems, and enforcement mechanisms such as disabling accounts.

2.2.4 Operational Resilience

This capacity area addresses how well a country or organization is postured to protect against, identify and characterize, respond to, and recover from a cyber incident affecting its key systems, data, or services, often while under duress. This includes provisions for critical systems protection—such as "crown jewel" identification, system and dependencies mapping, vulnerability assessments, physical diversity, and system/data back-up, as well as cyber threat intelligence capabilities and information sharing. It also addresses the capacity of key stakeholders to implement actions to compensate for and/or recover from the degradation, denial, or loss of operational capabilities—this is typically a combination of good design, adequate staffing/training, and well-exercised procedures.

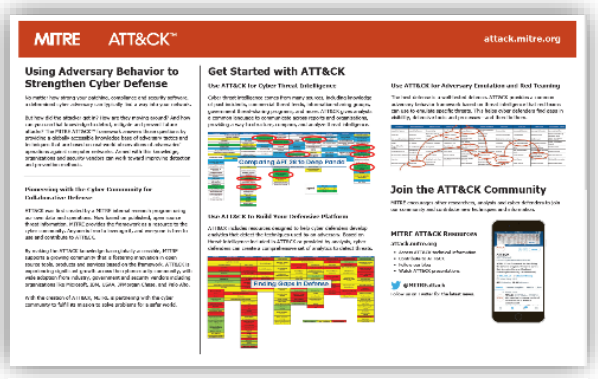


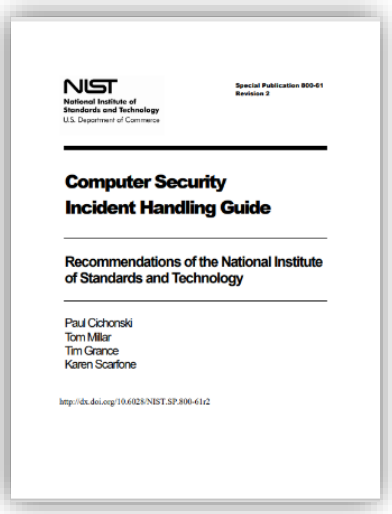
Figure 8: The ATT&CK Framework helps organizations improve resiliency by identifying and remediating risks

From a capacity building standpoint, some aspects of operational resilience are straightforward and affordable, while others are complex and expensive. For example, adding malware protections and encryption capability to essential systems and databases is relatively simple, whereas adding robust off-site back-ups and the skilled personnel to exercise those backup processes can be difficult. Similarly, when designing and implementing new systems, architectures, or critical infrastructure, it is a cost-effective best practice to ensure that security and resiliency provisions (including, in the case of critical infrastructure, manual overrides where feasible) are designed into the new system—these may include physical and virtual access controls, monitoring, encryption, segmentation, backup, failovers, redundant cooling, etc.—whereas adding these measures post-implementation is extremely costly and complex, as well as generally less effective.

It can be difficult for system owner-operators to convince decision-makers that the incremental resources required up-front to make a system more resilient are a good strategic investment, but it is important to make this case, as the costs—both political/reputational and financial—of incident recovery can be devastating. One resiliency initiative that is invariably worth the investment is ensuring all systems and software supporting critical systems and services (and their suppliers) are properly licensed, with vendor commitments and processes for vulnerability patching and updates. This includes devices that connect to these systems, such as wi-fi routers, desktop/laptop computers, printers, and mobile devices.

At the national level, it is worth looking at some of the creative operational resiliency solutions implemented by other countries—for example, Estonia's Data Embassies, which allow them to back up critical government systems and data on Estonian sovereign territory (embassies) in other countries, making it more difficult and politically hazardous for adversaries to attempt to compromise it. At both the national and organizational level, cloud services are increasingly used to improve resiliency in a cost effective manner—a reputable cloud service provider typically has both the highly trained, dedicated cybersecurity staff, and the resources and processes to secure and back up data that may be difficult for governments or non-ICT organizations to sustain. There are, of course, trade-offs involved in any strategic investment—strategy teams should conduct careful risk comparisons of possible resiliency initiatives.

2.2.5 Incident Response


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61 Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

The ability to detect, characterize, and respond to cyber incidents, including but not limited to attacks (human error and physical disaster/incident are also common causes of cyber incidents), is a significant goal in the cyber strategies of most nations and organizations. This capacity area includes situational awareness pertaining to key networks and systems, the sufficiency of trained cybersecurity personnel and appropriate devices/tools to detect the event, established procedures for reviewing logs and initiating incident checklists, the checklists or playbooks themselves—including procedures and contact information for incident communications and elevation to higher decision makers, information sharing mechanisms, in-house or on-contract responder capabilities, and the capacity of external key stakeholders to assist in response actions, including through partnerships.

Incident response is one of the capacity areas in which significant improvements can be made through policy and process—that is to say, without a large capital investment in technology. Although it is necessary to have certain technology capabilities associated with situational awareness, such as intrusion prevention/detection devices and network monitoring systems, much of effective incident response comes down to carefully considered and executed policies and processes, such as identifying in advance what kinds of activity constitute alarm signals, who is responsible for checking for those, and what are the steps required when an anomaly is detected. Merely instituting response checklists that clearly identify who to contact in a particular situation—including upstream decision makers, downstream customers or recipients of services, and stakeholder partners who may be able to verify or assist in responding to the problem—can make a substantial difference in an organization's incident response capacity.

Another key activity in incident response capacity building is the identification and elimination of stovepipes that hinder information sharing. These barriers exist across many governments and organizations—some culturally entrenched, and some inadvertent or undiscovered. Cyber incidents rarely stay constrained to a single set of constituents—rather, they tend to cross lines where data is shared, suppliers and consumers of services and data connect, affected services are provided outside of the organization experiencing the incident, and/or where leadership of a broader ecosystem—such as a Ministry, government, or corporation—is held responsible for the

activities of a single sub-unit. Moreover, particularly in government, different organizations typically have different cyber incident related authorities, such as response, investigatory, prosecutorial, operational, diplomatic, and defense roles that are likely to intersect and overlap in a significant incident. Clarifying these authorities in law or policy, deliberately establishing information sharing expectations and timelines, creating operational coordination mechanisms and procedures such as Security Operations Centers or Cyber Security Coordination centers, and ensuring stakeholders understand and will be responsive to appropriately authorized actions and directives anticipated in a cyber incident, are all examples of incident response capacity building measures that, though not simple, may be initiated at a relatively low cost and on a relatively short timeline with the appropriate resources and mandates in place.

2.2.6 Cybercrime Prevention & Prosecution

This capacity area addresses legislation, policy, training/awareness, and staffing specific to cybercrime (as opposed to regulatory or statutory laws/policy). It includes the ability to prevent and combat both cybercrime (including data theft, identity theft, destruction, or fraud) and cyber-enabled crime (such as extortion and human, drug, or weapons trafficking executed through cyberspace), and to ensure on-line protection for internet users—particularly children.

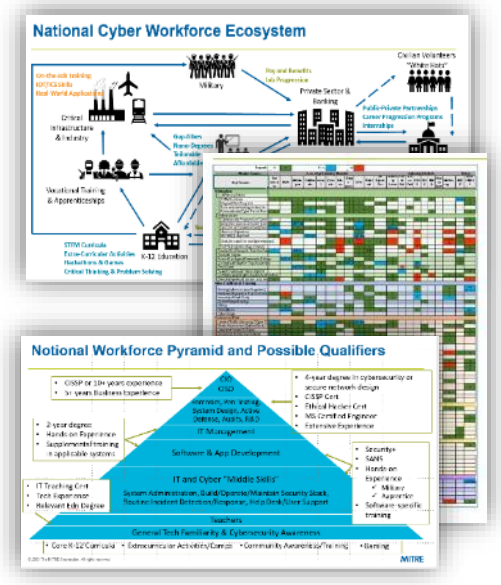
Cybercrime Prevention & Prosecution capacity encompasses defining, preventing, identifying, responding to, and prosecuting cyber-related crime. It also includes user/system owner awareness, training, and trusted relationships with law enforcement that support reporting and response. At the national level, it includes the capacity of law enforcement to detect and respond to cyber threats, as well as those capabilities required for cybercrime prosecution, such as electronic evidence handling, cyber-forensics, and judicial and prosecutorial training, as well as international and regional crime-fighting partnerships.

A lack of capacity in this area can present serious national problems, eroding trust in government, foreign investment, citizen safety and prosperity, economic security, and national security—specific best practices for creating the legislative capacity to deal with these crimes is detailed in the Budapest Convention on Cybercrime, the provisions of which should guide even those governments that have not formally acceded to the convention. At the organizational level, a lack of capacity in this area may manifest as insider perpetrated theft, fraud, or abuse—particularly in organizations entrusted with financial or identity management transactions—or as preventable outside compromises, as have occurred in numerous retail and commercial enterprises.

2.2.7 Cyber Workforce Development

Cyber Workforce Development is a significant (indeed, near universal) capacity building priority for both nations and organizations. Worldwide, the shortage of qualified workers in cyber- or ICT-related jobs is expected to exceed 3.5 million over the next few years, and this number is likely to grow as industries, services, and technologies continue to become more digitally reliant and interconnected, for example through a growth in 5G network and 'Internet of Things' (IoT) technologies. Across the board, in governments, industry sectors, and companies, employers are finding that they do not have enough qualified applicants for the jobs they post, while many potential employees either are not aware of or feel they are not suited to these jobs. Establishing skills-based job requirements and the programs to produce employees with those skills, is a major capacity building need nearly everywhere.

Cyber Workforce Development is a near-universal capacity building priority for both nations and organizations



This capacity area is one of the more complex, but also more fundamental strategic needs for both national governments and other organizations, comprising not only the supply of foundational digital skills suitable to the majority of cyber/ICT jobs (system/database administration, basic network security, user or helpdesk support, and first-level incident detection/response), but also training for both the technical and non-technical workforce, and the effectiveness of security awareness programs for users. At the national level, it includes the country's goals and capacity in cybersecurity workforce pipeline development, including primary and secondary school curricula and technology access, university and non-university (such as Academies) technical training/certification programs, and the policies needed to support those pipelines. At the organizational level, it includes the ability to recruit and retain digitally skilled talent, whether through local education options or internal programs such as apprenticeships and on-the-job training. Gap assessments in this area also address cyber workforce career progression and options for retaining workforce in key areas where salary incentives may be insufficient or unavailable.

Best practices in this capacity area include establishing a common lexicon among government, academia, and industry that can be used to identify common workforce needs and develop partnerships for increasing required skills. The US' National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) program has developed a taxonomy of cyber-related skills and associated position descriptions as an enabler for describing and developing appropriate training programs and ensuring effective requirements communications among training providers, trainees, and employers. The US government and many major employers both in and outside of the ICT sector recommend using the NICE framework to ensure job descriptions are skills-focused (rather than degree, experience, or

certification-focused) and to create a common understanding of broad cyber workforce requirements.

In addition, research has repeatedly shown that hands-on training programs for entry-level training, re-skilling, and up-skilling are among the most effective programs for growing a cyber workforce, and that these programs can and should be available below University level, at accessible locations/times, ideally with a grant/stipend or work-study employment arrangement that allows trainees to meet their basic economic needs while pursuing these skills. For governments, which can rarely afford to pay competitive wages for highly skilled cyber workers, public-private partnerships, programs such as cyber "Reserves" and scholarships-for-service initiatives, and incentives like defined career progression tracks, continuing training opportunities, and appeals to patriotic service can help attract, develop, and retain skilled workers.

2.2.8 Public Awareness & Culture of Cybersecurity

Digital literacy and public or user awareness of cyber vulnerabilities and threats is a major component of cyber capacity in that its lack creates opportunities for cyberattacks, disinformation, and other compromises that can undermine national and economic security, reputation, trust, and user safety. This capacity area addresses the awareness basic cybersecurity risks and best practices on the part of non-technical users or the public as an essential component of a digital development. The higher a nation's or organization's aspirations about leveraging cyber technologies and services, and/or the greater its reliance on e-services and ICT, the more advanced its cybersecurity culture must be.

At the national level, Public Awareness comprises the basic education, strategic messaging, and human behavior components of developing a cyber-aware citizenry, including on-line protection programs in primary schools, public service announcements or campaigns at the national or local/community level, and, increasingly, programs that help citizens identify and resist or counter disinformation and social media manipulation. Such programs may address how users can secure their personal information and devices, protect their identity and financial information, interact securely with vendors over mobile devices, avoid scams and predators, and find credible information sources to counter dubious or false content online. At the organizational level, awareness programs are more likely to focus on non-technical employees and customers, and to address issues like cyber hygiene best practices, identifying phishing attacks, and the importance of knowing and complying with organizational security policies pertaining to appropriate internet usage, device connections, file downloads, and so forth. At both the national and organizational levels, clear and consistent messaging and periodic training that relate cyber security to individual financial, privacy, and safety concerns are often key initiatives.

2.3 The importance of Partnerships

One more enabling activity is key to cyber capacity-building: Partnerships. This activity is not addressed as a separate capacity area because it is an essential contributor to *every* capacity area. It includes both internal and external partnerships that support the entity's strategic goals, including commitment to creating robust internal partnerships among agencies and offices; public-private partnerships between government and key industry leadership; and international partnerships, between government and international or regional organizations and donor entities. Appropriate partners will vary in different capacity areas and in different contexts—for example, information sharing partnerships with internal stakeholders such as suppliers and business components will be essential to incident response, whereas international partnerships may be more relevant to countering cybercrime, and civic partnerships will play a larger role in workforce development and public awareness.

Partnerships are an essential contributor to every cyber capacity area.

It is important to establish mechanisms through which to engage strategic partners. At the organizational level, this may take the form of an advisory board or working group. At the national level, it may be a subset of a national cyber coordination center or function. When assisting other governments in developing their strategies, it typically is managed through an interagency Cyber Working Group hosted by the US Embassy, which ideally interfaces with an analogous group in the partner government. **Establishing these mechanisms is a critical part of Strategic Foundations**, since in any cyber capacity building effort, if all major stakeholders are not represented in these forums, the cyber strategy and its implementation are less likely to meet the expectations of all parties, resulting in disillusionment, stakeholder frustration with the process, and waste of resources.

2.3.1 Public-Private Partnerships

Cyber capacity building, whether at the national or organizational level, often necessitates partnerships between government—in the form of regulatory, policy-making, law enforcement and intelligence entities—and the private sector, in the form of ICT companies and internet providers, cybersecurity firms, infrastructure owner-operators, software vendors, suppliers, and customers. In some cases, it also involves interactions with the civil sector through education and training providers, watchdog groups, community services and non-governmental organizations (NGOs). Having representatives from these potential partners participate in the strategy development process generally helps create a more complete and relevant cyber strategy by bringing in different perceptions of risk, opportunity, and interoperability/access concerns. It also can help lessen or preclude resistance during implementation by ensuring these partners understand the deliberations that shaped the strategy, informed its priorities, and guided necessary tradeoffs. ***Many leaders enter the strategy process convinced that it will be more successful if they complete the strategy first and then "sell" it to constituents and partners, but this is rarely the case.*** Whether internal or external, other stakeholders are more likely to accept and even embrace a strategy—even one that constrains their activities, requires difficult choices, or fails to fulfill their particular priorities—if they participated in the process and know their views were considered, though their wishes may not have been fulfilled.

Many leaders enter the strategy process convinced that it will be more successful if they complete the strategy first and then "sell" it to their stakeholders, but this is rarely the case.

2.3.2 Partnering with Foreign Governments

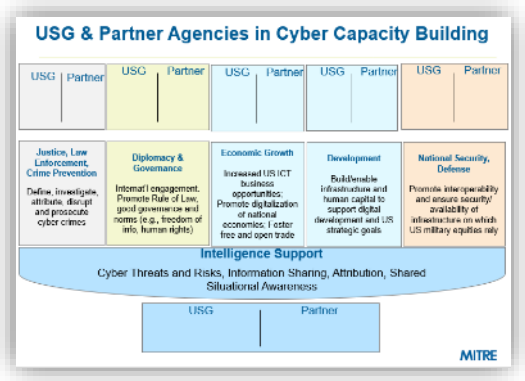


Figure 9: Embassy Interagency Cyber Working Group Model

For US government entities engaged in cyber strategy development, whether internally or with foreign partner governments, several areas of partnership related to national-level cyber strategy should be considered—law enforcement, diplomatic, economic, commerce/development, and national security agencies all have unique roles and authorities in cyberspace, as does the intelligence community, which is essential to threat awareness. Cyber capacity building at the national level is extremely complex, requiring the skills of the entire Embassy team, to include Foreign Commercial Officers, law enforcement and judicial representatives; defense and development representatives; and intelligence community members; and multiple individuals or implementers with expertise across all eight of the key capability areas, as well as some enabling functions such as organizational change and strategic communications. Diverse Embassy US Cyber Working Groups not only improve deconfliction and unified effort, but can also serve as a model of effective interagency coordination during engagement with their foreign counterparts. **Ideally, the stakeholder group engaged by the US Cyber Working Group or its representative(s) will form the core of this interagency coordination group**, reinforcing personal relationships and providing a common convening mechanism and opportunitiy that often does not exist in the partner government's normal operations. Through this US-partner nation relationship, the Cyber Working Group can offer insights, guidance, and assistance as appropriate across the strategic landscape. In doing so, it may also choose to leverage the resource and expertise of other US and international assistance partners who can add valuable expertise.

2.3.3 Partnering with other Cyber Capacity Building Organizations

While US interests, funding appropriation processes, specific operational needs, resource constraints, technology or training limitations, competing priorities, and other factors may drive engagement in particular capability areas, other **partners are available and eager to assist in various aspects of cyber capacity building** and should be considered for inclusion in cyber strategy development and implementation. As examples, at the national level, the Council of Europe offers training for countering cybercrime supporting law enforcement personnel, prosecutors, and the judicial sector up to and including the national Supreme Court; the US Department of Justice offers orientation seminars and sometimes law enforement training; the Global Forum for Cyber Expertise acts as a clearing house for capacity building projects, matching donors, implementers, and requesters, various nations and the World Bank support infrastructure and e-services development and Secure Elections assistance, and in some countries the US Department of Energy offers assistance in cybersecurity certification training for critical infrastructure operators. **It has proven very helpful in partner nation engagements to establish regular situational awareness and deconfliction meetings with all of the assistance provider organizations on a regular basis**—at least annually, but better semi-annually or

Approved for Public Release Case #20-2683.

quarterly—to discuss assistance efforts in order to avoid duplication and identify new opportunities for mutual support.

For organizations, some industry sector members may be willing to support 'best practices' training focused on common business applications, and various national and international non-governmental organizations and non-profits offer programs aimed at social media, public awareness and educational curricula. This list is not exhaustive—more interested parties with particular expertise and resources emerge constantly. **At both the national and organizational levels, it is often useful to meet with representatives of academia and local industry providers of various cyber-related services**, including critical infrastructure, communications, and banking where those are not state-owned, as well as cybersecurity training, IT services, and data services providers, and local system or application developers and employers in industries focused on technology. All of these may offer insights into the local cyber ecosystem, and many are eager to engage with government in improving cyber capacity, sharing information, and combatting cyber threats but may not have channels in place through which to offer or pursue those partnership opportunities.

3 CSDI Tools and Approaches

In implementing the CSDI framework, it has proven most effective to employ in-person interviews, discussions, workshops, and engagements that maximize the inclusion of stakeholders. The intent of this interaction is to foster trust in the strategy development and facilitator team and enthusiasm for participating in the planning process. These are essential elements to gaining an accurate and relevant understanding of a cyber strategy needs and, conversely, to avoid perceptions of a one-size-fits-all approach. This is particularly important in cyber strategy development because cyber-related technologies and processes almost always cross functional, organizational, spatial/geographic, and mission lines where different stakeholders' inputs have a significant effect on successful implementation. Personal engagement also helps defuse any tendency among organizational leadership to feel defensive in the face of external evaluation and technical advice. Such defensive reactions can potentially undermine the effectiveness of the engagement by prompting decision-makers to limit access to the right stakeholders, participate only superficially, and/or lose interest.

One key aspect of facilitator engagement is to demonstrate an interest in and awareness of the organization's individual circumstances, and a desire to leverage that understanding to assist in the creation of a strategic plan

One key aspect of the facilitator's engagement is to demonstrate an interest in and awareness of the country or organization's individual circumstances and needs, and a desire to leverage that understanding to assist in the creation of a reasonable strategic plan, thereby establishing the foundation for a productive long-term relationship that will support a more nuanced approach to strategy implementation. Accordingly, most of the CSDI tools and approaches are based on Design Thinking principles, which are based on ideation and prioritization/selection techniques aimed at soliciting the broadest set of perspectives feasible in order to identify solutions that both meet underlying needs and gain stakeholder buy-in.

That said, it is not always possible to engage in person, and some engagements or strategy development efforts must be conducted remotely, virtually, or through intermittent "check-ups"

augmented by supplementary material on best practices or alternative approaches. Some of MITRE's ever-growing library of tools, guides, and methods for developing and implementing cyber strategies include the following, which are available upon request:

Assessments:

- Cyber Capacity Assessment Stakeholder Sruvey
- SOC/CSIRT Capacity Survey
- Various vulnerability assesssments (these require hands-on access to networks and range from basic policy/compliance to penetration testing, mission impact, and Crown Jewels assessments – the latter can take up to several weeks to accomplish)
- ATT&CK Assessment/mapping

Interactive Workshops:

- National Cyber Context and Goal Setting (.5-1 day)
- National Cyber Risk Management (1-3 days)
- Industrial Control System Risk Management (1 day)
- National Cyber Strategy Development (1 day)
- Developing and Prioritizing Implementation Approaches (1-2 days)
- Operational Coordination & Incident Response (1-3 days)
- Developing Key Partnerships (.5 days)
- Engaging the Private Sector in Cyber Capacity Building (.5 day)
- Organizational Change (.5-3 days)
- Strategic Communications & Public Awareness (.5-1 day)
- Approaches and Considerations for Workforce Development (.5-2 days)
- USG Assistance in Partner Nation Capacity Building (for Embassy Cyber Working Groups - .5-1 day)
- Countering Cybercrime (.5-1 day)
- Building NIST CSF Profiles (2-3 days)
- National Cyber Workforce Development: Public-Private Partnerships (2-3 days)

Tabletop Exercises:

- Operational Coordination for Incident Response
- National/Regional Coordination and Considerations for Incident Response
- Sector-Specific Incident Response
- Transnational Cybersecurity Threats and Considerations for Response

Guides:

- 10 Steps to Planning Your Cyber Strategy
- Considerations in Cloud Services Migration
- Ministry/Department Cyber Strategy in 12 Months
- National Cyber Strategy in 24 Months
- Competencies of a Successful Government Chief Digital Officer
- Considerations in Implementing the NIST Cyber Security Framework
- Improving National Cyber Operational Resiliency: Key Steps
- MITRE National Cyber Workforce Development Framework

Supporting Resources:

- 5G Risks Infographic
- 8 Preparatory Questions and Resources Workbook
- Interactive Risk Assessment Workbook
- Applying the Risk Management Process Worksheet
- Enabling Capabilities (Roots & Fruits) Worksheet
- NIST CSF Implementation Timeline InfoGraphic
- Cyberspace as a Key Policy Driver (paper)
- Organizational Cyber Strategy Development in 12 Months Infographic
- Role of a Government Chief Digital Officer Infographic
- Vulnerabilities-Attacks Map Handout
- Cognitive Biases in Risk Assessment Handout
- Overview of Threat Actors/Techniques Handout
- Evaluating National Cyber Incident Consequences
- Comparative Survey: International Approaches to Interagency Cyber Cooperation (paper)
- Establishing a National Cyber Coordinator (Paper)
- Generic Cybesecurity Governance Framework (Talking Paper)
- CISA (DHS) Election Infrastructure Questionnaire
- Cyber Resiliency Design Principles (Technical Paper)

While many of these tools and workshops require training to use effectively, cyber strategy development teams or outside facilitators can use some of them to jump-start internal or partner-nation discussions about cyber capacity development, with or without MITRE assistance. In doing so, it is strongly recommends the US Embassy or other outside facilition team mirror the desired stakeholder composition to the greatest degree possible. **For national-level engagements**, **the facilitation team will be most effective when comprised of representatives from across the US government, representing national security, diplomacy, commerce/economic interests, law enforcment, development and assistance, political-military liaisons, and foreign service officers.** For organizational assistance, experts in the organization's various mission areas participate in early ideation sessions—for example, health care, financial services, law enforcement, energy, critical infrastructure, etc.

4 Conclusions

To take advantage of the opportunities and mitigate the risks of global connectivity, countries and organizations must understand their risk/opportunity context and actively integrate their technological development with their broader strategic goals. Building capacity in cyberspace requires mechanisms to establish a security and economic development environment that is reliable, interoperable and secure; that recognizes the need for coordinated efforts among multiple stakeholders to achieve goals; and that enables transparent governance, effective action, and growth. The CSDI Framework was developed to help countries and organizations create this environment, and to assist partners in narrowing cyber capability and performance gaps, reduce cyber-related risks, and foster better cooperation in cyberspace.

5 Summary of Appendices

Appendix A. Evaluation of National Cyber Strategy Guides and Indexes. Material that explains the indicators that make up the CSDI Framework and outlines existing methods of cyber strategy development. Includes references to materials that support and complement CSDI Framework.

Appendix B. National Cyber-Related Indexes & Related References. Provides analysis of several cyber maturity and capacity indexes produced by various regional, international, academic and consultant entities.

Appendix C. Additional Resources. Provides a list of US and international resource that FSOs and partner nation stakeholders may find useful in cyber strategy development and implementation.

Appendix D. MITRE Cyber Workforce Development Framework Overview. Provides an overview of MITRE's National Cyber Workforce Development Framework, addressing key findings, recommendations, and approaches.

Appendix A: National Cyber Strategy Development Guides

This appendix is intended to assist strategy teams and field personnel in quickly understanding the approaches, strengths, and weaknesses of several well-known cyber strategy and capacity development guides used to assist countries in their national cyber strategy development. The publications listed are a representative, not exhaustive list of the products available to assist in cyber strategy development.

A.1 Cooperative Cyber Defense Center of Excellence (CCDOE): National Cyber Security Framework Manual (2012)

The CCDCOE *National Cyber Security Framework Manual* is focused on cybersecurity as a component of national security, defining "national cybersecurity" as the security of a nation's online environment. It argues that the process of drafting a national cybersecurity strategy must navigate a complex public policy environment while addressing threats that may be political, technological, legal, economic, managerial or military in nature, or can involve other disciplines appropriate for risks. The authors explain that the four levels of government - political, strategic, operational and tactical/technical - each have their own perspectives on National Cybersecurity and give examples of relevant institutions, from top-level policy coordination bodies down to cyber crisis management structures and similar institutions. Its approach is academic and discursive rather than prescriptive. Academic in tone and intent, it is most useful as an introduction to the complexity of national cybersecurity policy in terms of balancing 'Five Dilemmas':

- Stimulating the Economy vs. Improving National Security
- Infrastructure Modernization vs. Critical Infrastructure Protection
- Private Sector vs. Public Sector
- Data Protection vs. Information Sharing
- Freedom of Expression vs. Political Stability

A.2 The Potomac Institute: Cyber Readiness Index 2.0 (CRI)

The Potomac Institute for Policy Studies' *Cyber Readiness Index 2.0* (CRI) is designed to inform national leaders on the steps they should consider when protecting their increasingly connected countries and potential GDP growth by evaluating each country's maturity and commitment to cybersecurity and resilience. CRI 2.0 examines one hundred twenty-five countries that have embraced, or are starting to embrace, ICT and the Internet and then applies an objective methodology to evaluate each country's maturity and commitment to cybersecurity using over 70 unique data indicators across the following seven elements:

1. National strategy
2. Incident response
3. E-crime and law enforcement
4. Information sharing
5. Investment in research and development (R&D)
6. Diplomacy and trade
7. Defense and crisis response

While it examines in detail a considerable number of countries, it does so against generic objectives and criteria (a maturity model approach, rather than their unique contextual threats, ambitions,

resources and needs.

A.3 Oxford Global Cyber Security Capacity Centre: Cybersecurity Capacity Maturity Model, Revised Edition (2017)

The Global Cyber Security Capacity Centre's *Cyber Security Capacity Maturity Model* (CMM), Revised Edition is a widely used measurement tool that is not intended to offer explicit advice on how to formulate a national cybersecurity strategy, but rather to highlight existing strengths and shortcomings. The CMM considers cybersecurity capacity consists of five dimensions:

- Devising cyber policy and strategy
- Encouraging responsible cyber culture within society
- Building cyber skills into the workforce and leadership
- Creating effective legal and regulatory framework
- Controlling risks through organization, standards and technology.

In assessing these dimensions, Oxford ensures buy-in and representation of relevant interests by consulting multiple stakeholder groups, including the public and private sectors, civil society, and international partners. To develop a capacity-building strategy around their assessment, the model uses data and historical trends to predict risks and threats, and scenarios or exercises to illuminate a current picture of national cyber resilience. It also highlights metrics and measurement processes to inform policy planners and decision making.

A.4 European Union Agency for Network and Information Security (ENISA): National Cyber Security Strategy Good Practice Guide (2016)

ENISA's *National Cyber Security Strategy Good Practice Guide* builds upon the first, 2012 edition, and identifies a set of concrete actions to lead to a coherent and holistic national cybersecurity strategy. Written in part as a response to the European Commission's 2013 Network and Information Security Directive, the guide aims to define the areas of importance of cyber security strategies, help EU Member States to develop, manage, evaluate and upgrade their national cyber security strategy, identify the challenges, the lessons learnt and the good practices from the NCSS practices followed by EU Member States, provide useful recommendations for policy and decision makers, and contribute to the Commission's efforts towards an integrated pan-European cyber security strategy. It proposes a list of possible key performance indicators (KPIs) for each component of the strategy. The ENISA guide was prepared by surveying and interviewing public authorities, chief information security officers, chief information officers, security architects and other IT/cybersecurity experts from 17 EU member states about their experiences and recommendations for effective practices in developing, implementing, evaluating and maintaining strategies.

A.5 International Telecommunications Union (ITU): Guide to Developing a National Cybersecurity Strategy (2018)

The ITU *Guide to Developing a National Cybersecurity Strategy* offers a useful and comprehensive framework for aligning national security and economic goals with cybersecurity measures. It describes a complex lifecycle approach comprising nine cross-cutting enabling

principles, seven focus areas, and five phases, accompanied by lists of the stakeholders and key thought processes needed to accomplish each phase. The seven key focus areas are introduced as good-practice elements to make a strategy comprehensive and effective, and include: Governance; Risk Management; Preparedness and Resilience; Critical Infrastructure Services and Essential Services; Capability and Capacity Building and Awareness Raising; Legislation and Regulation; International Cooperation. The Guide also provides a thorough listing of reference materials to guide the reader in further research on any of the focus areas or key enablers. Its strengths as a thought piece include its emphasis on values and interests as the basis of strategy development and on the need to prioritize investments and resources by employing a risk management approach. It also offers case study vignettes throughout.

A.6 Microsoft: Developing National Strategy for Cybersecurity (2013)

Microsoft's *Developing a National Strategy for Cybersecurity* argues for the need to formulate, implement and continuously update a national cybersecurity strategy. It offers basic (and occasionally thin) recommendations on the direction and content of a strategy. It mostly focuses on basic technical, systemic and law enforcement aspects of cybersecurity, providing useful guidance to less cyber-advanced nations wanting to establish and enhance their fundamental cybersecurity posture. Not surprisingly, Microsoft is primarily interested in cybersecurity architectures and incident response capabilities. This interest leads to a focus on identifying systems of national importance; understanding what constitutes a national-level incident; and defining stakeholder roles and responsibilities in responding to such incidents—a practical approach to stakeholder engagement that many countries might find useful in overcoming bureaucratic or cultural hurdles to cooperation. It is based on broad international experience with cybersecurity challenges in different countries, and provides useful guidance to less cyber-advanced nations seeking to establish and enhance their fundamental cybersecurity while embracing international standards and principles of privacy and freedom of information, and promoting international cooperation in countering cybercrime, establishing certifications, and solidifying norms.

A.7 United Nations (UN) Resolution 64/211 (2009): Voluntary self-assessment tool for protecting critical information infrastructures

The self-assessment tool annexed to the UN General Assembly Resolution - *Creation of a Global Culture of Cybersecurity: Taking Stock of National Efforts to Protect Critical Information Infrastructures* - consists of eighteen recommendations to assist countries in their efforts to protect their critical infrastructures and strengthen cybersecurity.[3] The generic recommendations cover the main areas of national CIP policy and strategy formulation, but do not provide any explicit guidance on how to execute the measures or how to proceed with findings. It is specifically aimed at Member States and relevant regional and international organizations that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures, inviting them to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity.

[3] See also Resolution 57/239, January 2003 and Resolution 58/199, January 2004.

Appendix B National Cyber-Related Indexes & Related References

The following resources represent some of the national and regional indexes produced by various regional, international, academic and consultant entities to compare the capabilities and capacities of different countries in areas relevant to ICT development. Most are generally based on a "maturity" scale that is based on specific factors. These indexes typically facilitate peer-to-peer comparisons to inform and incentivize countries in their respective subject areas, and to guide and inform the country's and the development communities' capacity building investments. As such, they can be **helpful in identifying regional trends and exemplars and collectively, in providing some context for cyber capacity, indicating areas for improvement in each country, or motivating stakeholders to try and improve their country's standing capability areas with respect to their peers.** It should be noted that, national indexes merely present a "composite score" reflecting characteristics of concern to the developers at a moment in time.

B.1 Australian Strategic Policy Institute (ASPI): Cyber Maturity in the Asia-Pacific Region

The Cyber Maturity in the Asia Pacific Region is an easy-to-read and understand annual report that assesses the cyber maturity of 20 countries in that region. It provides a usable, quick-reference resource for considered, evidence-based cyber policy judgements pertaining to Asia-Pacific. ASPI aims to build a deeper understanding of regional countries' whole-of-nation approaches to cyber policy, crime, and security issues, and identify potential opportunities for engagement. With this analysis, governments and the private sector can gain context for tailoring engagement strategies to best fit existing levels of maturity in each policy area in each Asia-Pacific country. Additional aims include to:

- Lift the level of Australian and Asia–Pacific public understanding and debate on cybersecurity.
- Provide a focus for developing innovative and high-quality public policy on cyber issues.
- Provide a means to hold dialogues on cyber issues in the Asia–Pacific region.
- Link various levels of government, business and the public in a sustained dialogue on cybersecurity.

B.2 The Economist Intelligence Unit: Democracy Index

The Economists Intelligence Unit's *Democracy Index* is an annual study that provides a snapshot of the state of democracy worldwide for more than 150 independent states and territories. The Index provides scores on a range of indicators within five categories and classifies nations as of four types of democratic regimes – full, flawed, hybrid or non-democratic (authoritarian). Overall, the Index is intended to show how democracy fared globally, in any given year, focusing on specific issues of contextual importance such as the state of media freedom, which was the focus area in the 2017 report. In the context of cyber capacity building, this Index is useful as, when viewed together with measures of freedoms and economic factors, it can provide insight into a nation's overall social and free market environment, which can speak to factors that

are supportive of technical innovation. It also provides regional and global analysis, including the year's "champions" and "authoritarians."

B.3 Freedom House: Freedom on the Net Index

The Freedom House *Freedom on the Net Index* is an annual study of internet freedom around the world, measuring the ways that governments and non-state actors restrict rights online. It includes a well-explained methodology and features a ranked, country-by-country assessment of online freedom, a global overview of the latest developments, and in-depth country reports. In the context of cyber capacity building, the Freedom on the Net Index is indicative of the online human rights and freedom of speech posture of a given government, which translates to the usefulness and potential success of online platforms as well as a possible indicator of a government's propensity to use cybersecurity as a repression mechanism.

B.4 Heritage Foundation: Index of Economic Freedom

The *Index of Economic Freedom* is an annual data-driven research project by the Heritage Foundation that has been produced for more than twenty years. This Index is based on the idea that economic freedom is a critical element of human well-being and vital to sustaining a free society. In the context of cyber capacity building, a society that has reached a high level of economic freedom is likely indicative of a society that has room for the commoditization of technical research and development and mechanisms to bring innovation to market. The index scores 180 nations across thirteen indicators of economic freedom charted against other relevant data collections such as standards of living, GDP per capita and poverty reduction metrics, and then ranks nations numerically and assigns one of five labels – free, mostly free, moderately free, mostly unfree, and repressed.

B.5 International Telecommunications Union (ITU): Global Cybersecurity Index (GCI)

The ITU *Global Cybersecurity Index* (GCI) is a multi-stakeholder initiative to measure national commitment to cybersecurity across many industries and sectors. Each country's level of development is analyzed within five categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation. The result is a country-level index and global ranking of cybersecurity readiness. The GCI does not seek to determine the efficacy or success of a measure, but simply the existence of national structures in place to implement and promote cybersecurity. This index is based on a self-assessment by all ITU countries—as a result, some activities and achievements listed are only remotely related or irrelevant to the main questions.

B.6 International Telecommunications Union (ITU): ICT Development Index (IDI)

The ITU ICT Development Index (IDI) measures progress on ICT development in general and on the affordability of ICTs for individuals and communities worldwide. The ICT Development Index combines data concerning ICT access, use and skills in an overview assessment of national ICT ecosystems, while the ICT Price Basket (IPB) is concerned with affordability.

B.7 UN: E-Government Development Leaders Index (EGDI)

The UN World E-Government Development Leaders Index (EGDI) serves as a tool for decision-makers to identify their areas of strength and challenges in e-government and to guide e-government policies and strategies. The EGDI is a composite measure of three dimensions of e-government: 1) provision of online services, 2) telecommunication connectivity and 3) human capacity. The global e-government ranking, as derived from the EGDI, is not designed to capture e-government development in an absolute sense; but aims to give a performance rating of governments relative to one another.

B.8 World Economic Forum: Networked Readiness Index (NRI)

The World Economic Forum Networked Readiness Index (NRI) measures the propensity for countries to exploit the opportunities offered by information and communications technology (ICT). It is published as part of the annual Global Information Technology Report (GITR), regarded as the most authoritative and comprehensive assessment of how ICT impacts the competitiveness and well-being of nations. The index aims to understand the impact of ICT on national economic competitiveness, and to build and strengthen digital ecosystems as a key component of economic growth. The NRI rests on six principles: (1) a high-quality regulatory and business environment is critical to fully leverage ICTs and generate impact; (2) ICT readiness—as measured by ICT affordability, skills, and infrastructure—is a pre-condition to generating impact; (3) fully leveraging ICTs requires a society-wide effort (government, industry, and citizenry); (4) ICT use should not be an end—their impact on the economy and society is what ultimately matters; (5) the environment, readiness, and usage factors interact, co-evolve, and reinforce each other to form a virtuous cycle; and (6) the networked readiness framework should provide clear policy guidance.

Appendix C Additional Resources

C.1 U.S.-Sourced and U.S. Government-Endorsed Resources

Resource	URL	Descriptor	Appropriate Audience
United States Telecommunications Training Institute	http://ustti.org/	Tuition-free technical training in various operational telecommunications subjects	Technical Staff
The NATO School Courses	www.natoschool.nato.int/Academics	Listing of courses offered by the NATO School, includes operational level courses in cyber security	Technical Staff, Incident Responders
George C. Marshall Center Program on Cybersecurity Studies	www.marshallcenter.org/MCPUBLICWEB/en/nav-main-wwd-res-courses-pcss-en.html	A policy-focused, non-technical program that teaches senior leaders how to make informed decisions on cyber policy, strategy and planning	Policy Makers
ENISA Calendar of Events	www.enisa.europa.eu/events	Listing of current cybersecurity-focused lectures, conferences and activities hosted by ENISA	Policy Makers, Technical Staff, Incident Responders
OSCE Calendar of Events	www.osce.org/events	Listing of OSCE activities around the globe; includes ICT and cyber security-focused events	Policy Makers
UN Group of Governmental Experts Report (2015)	http://undocs.org/A/70/174	Report on developments in the ICT field in the context of international security focusing on building a "peaceful, secure, resilient and open ICT environment".	Policy Makers
UK Cyber Essentials Scheme	www.cyberstreetwise.com/cyberessentials/	Guidelines to provide businesses small and large with clarity on good basic cyber security practice	Technical Staff
NIST Cybersecurity Framework	www.nist.gov/cyberframework/	A framework for reducing cyber risks to critical infrastructure based on existing standards, guidelines, and practices	Policy Makers, Technical Staff
International Standards Organization (ISO) Standard 27001:2013	www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534	Standards that specify the requirements for establishing, implementing, maintaining and improving an information security management system	Technical Staff
International Standards Organization (ISO) Standard 15408-1:2009	www.iso.org/iso/catalogue_detail.htm?csnumber=50341	Standard that establishes the general concepts and principles of IT security evaluation	Technical Staff
North American Electric Reliability Cooperation (NERC) Standards	www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx	Standards used to secure bulk electric systems, including network security administration.	Technical Staff

	Forum for Incident Responders & Security Teams	www.first.org	Resources to help develop, operate, and improve incident management capabilities	Incident Responders
	StaySafeOnline	https://staysafeonline.org/re-cyber/cyber-risk-assessment-management/	A discussion of integrating cyber risk management into day-to-day operations	Policy Makers, Technical Staff
	5 Cybersecurity Questions for CEOs	https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf	Provides key questions to guide leadership discussions about cybersecurity risk management	Policy Makers
	ENISA Evaluation Framework for Cyber Security Strategies	www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies	An evaluation framework that provides a logic model and a list of possible cyber security key performance indicators (KPIs)	Policy Makers
	Freedom on the Net Report	https://freedomhouse.org/report/freedom-net/freedom-net-2017	Ranked, country-by-country assessment of online freedom, a global overview of the latest developments, as well as in depth country reports.	Policy Makers
	Institute of Electrical and Electronics Engineers(IEEE) Cybersecurity Resources	http://cybersecurity.ieee.org/	Digital library of IEEE publications on technical cybersecurity topics	Technical Staff
	Internet Governance Forum	www.intgovforum.org/multilingual/	A global multi-stakeholder platform facilitating discussion of public policy issues pertaining to the Internet	Policy Makers
	NIST Computer Security Resource Center	https://csrc.nist.gov/	Computer, cyber & information security guidelines, recommendations and reference materials	Policy Makers, Technical Staff, Incident Responders
	Carnegie Mellon SEI CSIRT Development & Training	www.cert.org/incident-management/	Resources to help develop, operate, and improve incident management capabilities	Incident Responders
	ICS-CERT Training	https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT	Listing of virtual and live training events on the topic of industrial control system computer emergency response	Technical Staff, Incident Responders
	MITRE Cybersecurity Resources	www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-resources	Computer, cyber & information security guidelines, recommendations and reference materials	Technical Staff, Incident Responders
	Forum for Incident Responders & Security Teams (FIRST)	www.first.org	Resources to help develop, operate, and improve incident management capabilities	Incident Responders
	ENISA Analysis and Recommendations on the protection of CIIs	www.enisa.Europeopa.eu/publications	Principles, processes and instruments to implement critical infrastructure protection	Policy Makers, Technical Staff, Incident Responders

	ENISA CSIRT Resources	www.enisa.Europeopa.eu/topics/csirt-cert-services	Resources to help develop, operate, and improve incident management capabilities	Incident Responders
	North American Electric Reliability Corporation	www.nerc.com	Principles, processes and instruments to implement critical infrastructure protection	Technical Staff
	The Financial Management of Cyber Risk	https://webstore.ansi.org/cybersecurity.aspx	The American National Standards Institute and the Internet Security Alliance framework for managing and reducing financial risk related to cyber attacks	Policy Makers
	Council of Europe	http://www.coe.int/en/web/cybercrime	Extensive assistance for cybercrime capacity building	Policy Makers, Judicial/Law Enforcement
	Risk Assessment	https://www.ready.gov/risk-assessment	US Dept of Homeland Security Risk Assessment Guidelines	Policy Makers, Technical Staff
	NIST Cybersecurity Framework	https://www.nist.gov/cyberframework	Link to NIST Framework for Improving Critical Infrastructure Cybersecurity and supporting resources	Policy Makers, Technical Staff, Incident Responders
	US-CERT Publications	https://www.us-cert.gov/security-publications	Publications that cover a variety of cybersecurity topics from setting up a computer to understanding the nuances of emerging threats	Policy Makers, Incident Responders
	US Department of Energy Cybersecurity Capability Maturity Model (C2M2) Program	https://energy.gov/oe/cybersecurity-critical-energy-infrastructure	A public-private partnership effort to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the grid	Policy Makers, Technical Staff
	US Department of Justice Computer Crime & Intellectual Property Section	https://www.justice.gov/criminal-ccips/cybersecurity-unit	White papers, documents and reports on the shaping of cybersecurity legislation and outreach to private sector to promote lawful cybersecurity practices.	Policy Makers, Judicial/Law Enforcement
	GFCE	www.thegfce.com	A global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building.	Policy Makers
	Good Practice Guide on Cooperative Models for Effective Public Private Partnerships	https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps	This guide classifies partnerships for security and resilience and addresses questions associated with creating and maintaining partnerships	Policy Makers, Incident Responders
	Desktop Research on Public Private Partnerships	https://www.enisa.europa.eu/publications	Collates information from the learning and experiences of existing public-private partnerships	Policy Makers, Incident Responders
	The Meridian Process	www.meridianprocess.org/	The Meridian Process aims to foster ideas and actions for governmental cooperation on	Policy Makers, Technical Staff,

			Critical Information Infrastructure Protection	
	Government of Canada, Get Cyber Safe	www.getcybersafe.gc.ca/index-eng.aspx	Resources for consumers and public online safety	Policy Makers, Judicial/Law Enforcement
	NOVA Labs Cybersecurity Awareness Videos	www.pbs.org/wgbh/nova/labs/lab/cyber/1/1	Resources for virtual cybersecurity training	Policy Makers
	Stop. Think. Connect.	www.stopthinkconnect.org	Public Awareness Campaign materials and resources	Policy Makers
	FBI Safe Online Surfing	https://sos.fbi.gov/	Resources to help teach children how to be safer on and offline	Policy Makers, Judicial/Law Enforcement
	FTC OnGuard Online	www.onguardonline.gov	Resources for consumers and public online safety	Policy Makers, Judicial/Law Enforcement
	National Initiative for Cybersecurity Careers & Studies (NICCS)	http://niccs.us-cert.gov	Resources for cyber education, training and talent management	Policy Makers, Technical Staff, Incident Responders
	NICE Cyber Workforce Framework	http://csrc.nist.gov/nice/framework/	Provides a common language and describes a set of tasks and skills to define, train, and recruit for cybersecurity work.	Policy Makers, Technical Staff, Incident Responders
	National Initiative for Cyber Education	https://www.nist.gov/itl/applied-cybersecurity	National-level resources for cybersecurity education, training, and workforce development	Policy Makers, Technical Staff, Incident Responders
	OAS Cybersecurity Awareness Campaign Toolkit	www.sites.oas.org/cyber/Documents	Public Awareness Campaign materials and resources	Policy Makers

C.2 Non-U.S. Sourced Resources

	Resource	URL	Descriptor	Appropriate Audience
	Commonwealth Approach for Developing National Cyber Security Strategies	www.cto.int/media/fo-th/cyb-sec	Provides practical advice and proposed actions for nations developing cyber security implementation plans	Policy Makers
	ITU Securing Information and Communication Networks: Section 2	www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22.1-2014-PDF-E.pdf#page=9	Best practices for Cybersecurity - Guide for the establishment of a national cybersecurity management system	Policy Makers, Technical Staff
	ITU-D Study Group Workshops 2014-2018	www.itu.int/net4/ITU-D/CDS/sg/index.asp?lg=1&sp=2014	Workshops for Member States and Sector Members to share experiences, present ideas, and achieve consensus on appropriate ICT strategies	Policy Makers
	ITU-D Cybersecurity Events	www.itu.int/en/ITU-D/Cybersecurity/Pages/Events.aspx	Listing of current cybersecurity-focused lectures, conferences and activities hosted by ITU-D	Policy Makers
	Diplomacy.edu Courses	www.diplomacy.edu/courses	Listing of current Diplomacy.edu courses, includes ICT and cyber security-focused courses	Policy Makers
	OAS Calendar of Conferences	www.apps.oas.org/oasmeetings/default.aspx?Lang=EN	Listing of conferences and activities hosted by OAS; includes ICT and cyber security-focused events	Policy Makers, Technical Staff, Incident Responders, Judicial/Law Enforcement
	Information Security Forum (ISF) Standards for Good Practice	www.securityforum.org/tool/the-standard-of-good-practice-for-information-security/	A comprehensive list of best practices for information security	Technical Staff
	International Society of Automation (IAS) Industrial Automation and Control Systems (IACS) Security	http://isa99.isa.org/ISA99%20Wiki/Home.aspx	A series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems	Technical Staff
	European Telecommunications Standards Institute (ETSI) Standards	www.etsi.org/standards-search#Pre-defined Collections	Standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies.	Technical Staff
	ENISA Evaluation Framework for Cyber Security Strategies	www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies	An evaluation framework that provides a logic model and a list of possible cyber security key performance indicators (KPIs)	Policy Makers
	Framework for Programming and	http://www.rand.org/content/dam/rand/pubs	Provides a basis to help prioritize and allocate resources for cybersecurity activities	Policy Makers

	Budgeting for Cybersecurity	/tools/TL100/TL186/RAND_TL186.pdf		
	European Commission European Programme for Critical Infrastructure Protection	http://Europe-lex.Europeopa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF	Principles, processes and instruments to implement critical infrastructure protection	Policy Makers, Technical Staff, Judicial/Law Enforcement
	CyberGreen	https://www.cybergreen.net/	Training Materials for Risk Management and Operational Resilience	Policy Makers, Technical Staff
	APNIC Training Courses	https://training.apnic.net/courses	Technical and Incident Response tutorials for CSIRTs or similar entities	Technical Staff, Incident Responders
	ENISA Analysis and Recommendations on the protection of CIIs	www.enisa.Europeopa.eu/publications	Principles, processes and instruments to implement critical infrastructure protection	Policy Makers, Technical Staff
	ENISA CSIRT Resources	www.enisa.Europeopa.eu/topics/csirt-cert-services	Resources to help develop, operate, and improve incident management capabilities	Policy Makers, Incident Responders
	European Commission European Programme for Critical Infrastructure Protection	http://Europe-lex.Europeopa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF	Principles, processes and instruments to implement critical infrastructure protection	Policy Makers, Technical Staff
	Family Online Safety Institute	www.fosi.org	Resources for online child safety	Judicial/Law Enforcement
	iKeepSafe	www.ikeepsafe.org	Resources for digital citizenship and online child safety	Judicial/Law Enforcement
	National Center for Missing & Exploited Children Netsmartz	www.netsmartz.org	Resources to help teach children how to be safer on and offline	Judicial/Law Enforcement
	G8 24-7 High Tech Crime Network	http://www.oas.org/juridico/english/cyb20_network_en.pdf	Points of contact in participating countries that require urgent assistance with investigations involving electronic evidence	Judicial/Law Enforcement
	Securing Cyberspace Through Public-Private Partnerships	https://www.csis.org/analysis/securing-cyberspace-through-public-private-partnerships	An info paper which presents and analyzes four public-private partnership models and offers a strategy for implementation for one of the models	Policy Makers, Incident Responders
	Good Practice Guide on Cooperative Models for Effective Public Private Partnerships	https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps	This guide classifies partnerships for security and resilience and addresses questions associated with creating and maintaining partnerships	Policy Makers, Incident Responders

	ITU Toolkit for Cybercrime Legislation	http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf	A toolkit that addresses the need for cybercrime legislation that is globally applicable	Judicial/Law Enforcement
	UNICEF "We Protect" Initiative	http://www.weprotect.org/	Resources for protecting children from exploitation online	Judicial/Law Enforcement
	UNODC Comprehensive Study on Cybercrime	http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf	UN-directed report on study aimed at strengthening national responses to cybercrime, including lessons learned and recommendations	Policy Makers, Judicial/Law Enforcement
	Interpol	http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime	Network of police in 190 member countries. Provides research, training techniques, and policing tools to combat cybercrime	Judicial/Law Enforcement
	Virtual Forum Against Cybercrime	https://www.cybercrimeforum.org/index.jsp	Partnership between Korean Institute of Criminality and UNODC provides training, resources, and access to a worldwide network to help combat cybercrime	Judicial/Law Enforcement
	Internet Watch Foundation	www.iwf.org.uk	Hotline for reporting criminal online content	Policy Makers, Judicial/Law Enforcement
	Better Internet for Kids	www.betterinternetforkids.eu	Resources for online child safety	Judicial/Law Enforcement
	OAS Cybersecurity Awareness Campaign Toolkit	www.sites.oas.org/cyber/Documents/2015%20OAS%20-%20Cyber%20Security%20Awareness%20Campaign%20Toolkit%20(English).pdf	Public Awareness Campaign materials and resources	Policy Makers
	Desktop Research on Public Private Partnerships	https://www.enisa.europa.eu/publications/copy_of_desktop-reserach-on-public-private-partnerships	A research study which collates information from the learning and experiences of existing public-private partnerships	Policy Makers, Incident Responders
	Council of Europe	http://www.coe.int/en/web/cybercrime	Home of the Budapest Convention and extensive assistance for cybercrime capacity building	Policy Makers, Judicial/Law Enforcement
	CSIAC Information Awareness Videos	www.csiac.org/series/information-awareness-videos/	Resources for virtual cybersecurity training	Technical Staff, Incident Responders

	Proteccion Online	www.proteccionon line.com	Spanish-language resources for consumers and public online safety	Policy Makers, Judicial/Law Enforcement
	ENISA Cyber Awareness	https://www.enisa.europa.eu/media/news-items/cyber-awareness-material_en.pdf	Provides cyber awareness materials such as educational materials, posters, videos, and exercises	Policy Makers

	Resource	URL	Descriptor	Appropriate Audience
	Cyber Streetwise	https://www.cyberstreetwise.com/	Provides resources to improve the online safety behavior and confidence of consumers and small businesses	Policy Makers, Judicial/Law Enforcement
	EU Calendar of ICT Events	www.eu-events.eu/categories-menu/ict.html	Listing of current ICT-focused lectures, conferences and activities hosted by the EU	Policy Makers
	Geneva Center on Security Policy Cyber Security Courses	www.gcsp.ch/Courses	Filtering on Cyber Security provides a listing of GCSP-hosted training	Policy Makers
	ASEAN Regional Forum Calendar of Events	http://aseanregionalforum.asean.org/events.html	Listing of ASEAN Regional Forum activities; includes ICT and cyber security-focused events	Policy Makers

Appendix D National Cyber Workforce Development

D.1 Overview

One key element in MITRE's Cyber Strategy Development and Implementation framework is the need for modern organizations to develop and retain cyber and ICT human resources with the skills and training necessary to support key systems and services.

This framework was developed in response to a growing awareness of the degree to which workforce shortfalls constrain cyber strategy implementation and capacity building—many organizations with well-founded cyber strategies simply do not have sufficient trained ICT personnel to sustain them. Reasons for this vary, but may include:

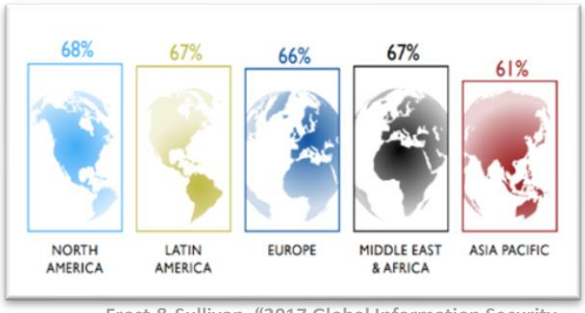
- The local economy has insufficient demand for cyber skills to drive adequate sourcing through training and education programs—local employers may need to re-skill their current workforce or attract new ICT workers, but that signal is not strong or coherent enough for the market to respond
- Local youth and those entering the workforce—particularly women—do not recognize cyber skills as something desirable and attainable
- There are significant numbers of skilled ICT workers, but they are concentrated in a few higher paying industries or companies—other employers such as government cannot compete
- Regional competitors draw the available cyber and ICT talent with higher paying jobs, a stronger economy, and/or more favorable working conditions (brain drain)
- There are training opportunities and programs available, but they are not well matched to the needs of local employers, including government
- Employers have access to entry-level ICT workers to support various aspects of their business processes, but do not have formal internal on-the-job training programs to "upskill" those workers
- Key employers, such as government, can attract entry-level workers through grants and similar programs but do not have the means—including in some cases policies or authorities—to provide incentives that can help attract and retain skilled cyber workforce

Workforce drivers and constraints, as well as potential development and training partners, differ among organizations and localities. This workforce development model takes a contextual, whole-of-ecosystem, partnership-focused approach to aligning cyber workforce training opportunities to employers' needs. It also addresses the need for a common lexicon among training and education providers and employers, including but not limited to government, that can help define and standardize demand for key skills so that appropriate recruitment, training, and retention programs can be developed. This framework uses the US National Institute of Standards and Technology's National Initiative for Cybersecurity Education (NICE) model as its notional common lexicon.

D.2 Workforce as a Key Capacity Enabler

Virtually every sector of a modern economy is becoming reliant on information and communications technologies (ICT)—security of these systems and data is a key component of economic success.

By 2022 the number of unfilled cybersecurity jobs worldwide is expected to have grown **350%** over 2013 requirements, topping **3.5M vacancies worldwide.** Our research shows current programs focused on university degrees and certifications are not aligned with employer needs—fewer than 1 in 4 applicants for IT/cyber jobs are qualified[4]—and while organizations have invested in cybersecurity technologies, they have not invested in the people to use them.



Frost & Sullivan, "2017 Global Information Security Workforce Study," (ISC)², Center for Cyber Safety & Education

Not only is this shortage limiting organizations' ability to leverage new technologies and compete in the digital economy, but inadequate cybersecurity training and staffing are top contributors to cyber breaches, undermining trust. **A recent year-long Information Systems Security Association survey (2017) of security executives found this skill shortage is:**

- Causing high rates of burnout and turnover (40%)
- Implicated in the top two factors perceived to contribute to breaches: inadequate training of non-technical employees, and inadequate cybersecurity staffing (the third is management failing to make cybersecurity a priority)
- Impacting their businesses (70%)—45% *know* they have experienced at least one security event in the past year; industry wide experience suggests the number is probably higher

D.3 Who is This Framework For?

Developed from data representing various city, state, national, and sector economies around the world, as well as ideas from cybersecurity, education, and economics subject matter experts, it is intended to be applicable to a wide range of entities:

- Nations transitioning to a digital economy or adjusting incentives and pipelines to increase investment in, and access to, cyber professionals
- City, State, or Regional entities focused on increasing high-tech employment
- Industry and academia seeking to grow a local talent pool
- Government agencies at all levels developing policy and/or legislation to incentivize cyber talent development and retention in key functional areas

D.4 What makes this Framework Valuable?

MITRE studied more than two dozen technology workforce development approaches used in different industry sectors and economies, at local and national levels around the world, as well

[4] MIT Technology Review October 2018,

as analyses by cybersecurity, technology, and labor and economics subject matter experts. We distilled **cyber workforce development insights, commonalities, needs, and best practices in 5 categories:**

- Traditional Education (K-12 and college/university)
- Other Training/Education approaches
- Employer Needs and Options
- Government Roles
- Cultural Factors

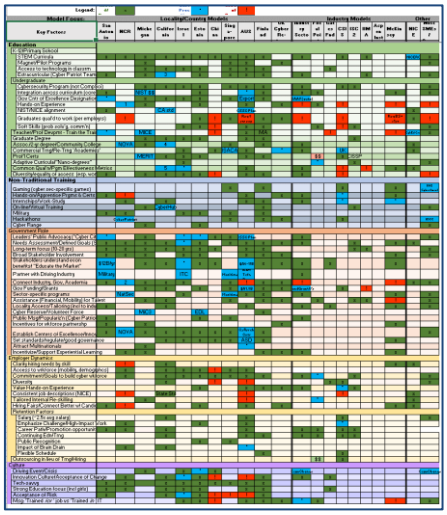
This research was then synthesized into a Framework focused on key areas and approaches for building cyber workforce capacity that can be tailored to a wide variety of ecosystems.

Some of our key findings, discussed in greater detail below, include:

- Non-university educated **job seekers are often not aware of ICT job opportunities**, and don't feel qualified to pursue them
- Perceptions that jobs involving digital skills are math-intensive, require high qualifications, and are limited to elite applicants **discourages many potential trainees, particularly women**
- **Employers' inaccurate assessments** of their cyber-related needs distort hiring practices and training incentives
- Current cyber workforce development paths focused on Universities and certifications do not adequately address the **vast need for practical "middle skills"** training
- **Public-private partnerships can be instrumental** in connecting industry, government, and academia in developing programs that meet local employers' needs
- Local, affordable, accessible **hands-on training** are key to accessing new arrays of potential employees, and can tailored to the needs of job seekers/employers
- A **common lexicon** (such as NICE) is important in identifying, describing, and building programs that can create the specific skills most needed in a modern digital workforce

This framework identifies best practices among both traditional and non-traditional workforce development approaches, as well as findings pertaining to education, employer requirements, the role of government, and the impact of innovation culture on developing a cyber-ready workforce. Finally, it provides some high-level recommendations for governments and employers, both for developing their own skills development programs, and for partnering with each other and with academia to establish a common set of skills-based competencies around which training programs and policies can be developed.

D.5 Methodology



To discover the major factors affecting cyber workforce development, MITRE researched a variety of different economies, at the city, US state, and national level, with different economic bases. All of these economies are in the process of either transitioning from an agricultural, industrial, or manufacturing economy to one that is more knowledge or IT-focused, or are adding additional industries and services that require more digital skills, such as banking, healthcare, communications, or direct support to the information technologies sector. We also examined several industry sectors that are modernizing and/or automating and therefore require re-skilling or upskilling of their current human resources, including the automotive manufacturing industry, industrial agriculture, aerospace, and higher education. Finally, we reviewed materials from subject matter experts in cybersecurity, economics, and education to ensure our set of potential approaches addresses the needs of all these stakeholders.

D.6 Summary of Research

The sections below overview key findings and insights into cyber workforce development at the national, local, and agency or organizational level.

D.6.1 "Educating the Market": The Role of a Cybersecurity Workforce in National Economies

While there is often a perception, driven in part by the prominence of the IT industry in the form of such massive corporations as Microsoft, Facebook, Google, IBM, et al., that digital skills are primarily the provenance of this sector, in fact virtually every industry and business today needs cyber-savvy workers to perform such routine functions as IT support, system administration, social media marketing, financial transactions, supply chain visibility and management, and support to business applications. However, many executives still do not prioritize cyber skills in hiring. Greater awareness among business owners of the potential economic impact of having (or not having) a skilled cyber workforce on their mission execution and/or profitability can help drive interest in investing in training programs and opportunities. For example, "smart factories" in which workers use apps, sensors, etc., are 10- 20% more efficient (through optimized capacity), experience a 20-30% reduction in costs (through improved resource accountability

Figure 10: In addition to foundational "middle skills," soft skills and emerging technologies will drive future cyber workforce needs

and logistics), and offer a 3-10% safer and more sustainable work environment as measured in environmental impact and accident rates.[5] However, to be "smart" a business needs an upgraded security infrastructure (such as firewalls, data encryption), supply chain integration and security, and good cyber security practices—all areas in which cyber-savvy workers can contribute at the worker, manager, human resources, and C-suite levels.

D.6.2 Sector Examples

According to McKinsey and Company research, in the early part of the 2010s, ICT contributed more than 10% of total GDP growth to countries like India, and in Africa, private internet investment could reach $62 billion annually by 2025, adding $300 billion a year to the Continent's GDP. In countries that have experienced this kind of expansion, companies with a robust internet presence were found to have grown twice as fast as those relying on traditional brick and mortar establishments. But ICT development stands to drive economic growth in other sectors as well. The following represent just a few examples of how ICT and cyber technologies contribute to industries in different sectors—**in each of these examples, the potential gains in productivity and effectiveness from ICT investments can only be realized with the help of individuals trained in the digital skills necessary to understand, implement, secure, and operate those technologies.**

D.6.2.1 Agriculture

ICT can help increase knowledge of agricultural improvements and innovations, along with providing market information and facilitating links to those markets. Mobile markets in particular have demonstrated the ability to provide better access to information, markets, and finance (e.g., credit or insurance). Nepal's Digital Strategy notes that ICT in Agriculture can help farmers:

- Leverage mobile applications for renting agriculture machinery and tools, and providing information on weather, market information, prices, and crops
- Use remote education to impart technical knowledge and best practices
- Improve productivity by using satellites, drones, and soil sensors to monitor and manage crop growth
- Use smart irrigation systems and equipment monitoring to minimize water loss, ensure higher irrigation efficiency, and optimize equipment resources
- Enable digital payments to farmers and intermediaries, and mobile credit platforms to provide loan facilities to underserved farmers
- Create an electronic trading portal which networks existing bazaars to create a unified national market for agricultural commodities
- Use logistic solutions and smart packaging (RFID sensors) to track shipments

Some examples of how ICT is contributing to agricultural economies include:

- Esoko, a mobile tool developed in Ghana and now used by individuals in 15 countries, provides users with **agricultural market information** like commodity prices and weather to help farmers to improve productivity and sell their products at the right price,

[5] Dupress.deloitte.com/smart-factory

the right place, and the right time. According to a World Bank report, farmers in Ghana using the app increased their revenue for maize, nuts, and cassava by 10 percent.

- Sri Lanka's e-Dairy helps farmers earn up to $262 more a year for each of their calves by providing **veterinary and extension services delivered by mobile phones**. Qualified veterinarians are available for consultation from across the country, without the previous need to travel long distances to remote areas.
- Tea growers in Kenya have reported average income growth of 9 percent—about $300 a year—by using Virtual City. This app provides information to buyers of tea, coffee, and cotton and allows farmers to receive **faster and more accurate pricing**, along with functions to **facilitate sales**.
- ICT sensors have **increased irrigation efficiency** in Egypt, increasing crop yield by 20 percent. By utilizing ICT, large and medium scale farmers can water crops only when needed. This has not only decreased the water needed, but also increased the yield, as crops receive the precise water needed at the right time.
- Livestock production is a widespread agricultural activity in Africa. For many of these farmers, the loss of a single animal, either through theft or separation from the pack, can be a huge financial loss. In Namibia, the use of radio frequency identification (RFID) **tracking of livestock** attempts to provide a mechanism for increasing traceability of important commodities like these.
- In the US, ICT is used in industrial agriculture to **optimize irrigation, fertilizer and pesticide applications**, to **remotely control farm machinery** using GPS coordinates, and to provide remote troubleshooting and software upgrades to that machinery.

D.6.2.2 Health Services

Investment in ICT has the potential to reform health systems, extend services to underserved areas, and reduce waste and redundancy. The use of ICT to provide remote diagnosis, treatment, and education could address the remoteness of patients in rural clinics that are often difficult to reach and to staff. These technologies have also proven to be a valuable tool in tracking, monitoring, and limiting the spread of disease outbreaks. Some specific examples of the role of ICT in modernizing healthcare include:

- In Mozambique, a program providing daily SMS **medication reminders** to patients led to 90% of tuberculosis patients taking all scheduled medication on time (up from 22%).
- Small pilots have shown the potential to increase **payments for health care services**. Paga, a mobile payments company, launched a mobile collection service for a hospital in Nigeria and in two months, the hospital managed to collect the same amount as in the previous 12 months.
- The PING Disease Surveillance and Mapping Project has created a mobile phone app that allows health facilities in Botswana to submit **reports on disease outbreaks (with GPS coordinates)** to the Ministry of Health. The system sends a text message to facilities nearby to alert them, driving a 365% increase in prompt reporting.
- The African Medical Research and Education Foundation (AMREF) in Kenya launched an e-learning program for nurses to access **continuing education training**. The tool has enabled the training facility to expand training from 100 enrollees a year to more than

4,500. Additionally, since healthcare professionals no longer need to travel to a single site, time away from their patients was drastically reduced.

D.6.2.3 Financial Services

Many citizens in rural areas do not have access to traditional banking options. ICT is likely to be a huge accelerator of financial inclusion, bringing banking and credit options to the underserved, who may live far away from a bank or ATM. Studies suggest that with the right technology solutions in place, more than 60 percent of Africans could have access to banking services by 2025, and more than 90 percent could use mobile wallets for daily transactions and remittances. According to McKinsey and Company, revenue from mobile financial services could increase from less than $1 billion today to $19 billion by 2025, and productivity gains in the sector are anticipated to total $8-10 billion. As just one example of how ICT contributes to the financial services sector, M-PESA, a mobile money transfer and microfinance service, allows users to **send and receive money securely**. Largely due to these services, the number of active bank accounts in Kenya more than quadrupled between 2007 and 2012. In 2012, transactions through M-PESA accounted for 20 percent of Kenya's national GDP, and by the end of 2016, mobile money accounts through services such as MTN Mobile Money and Ghana's KwikAdvance in West Africa totaled 83 million.

D.6.2.4 Education

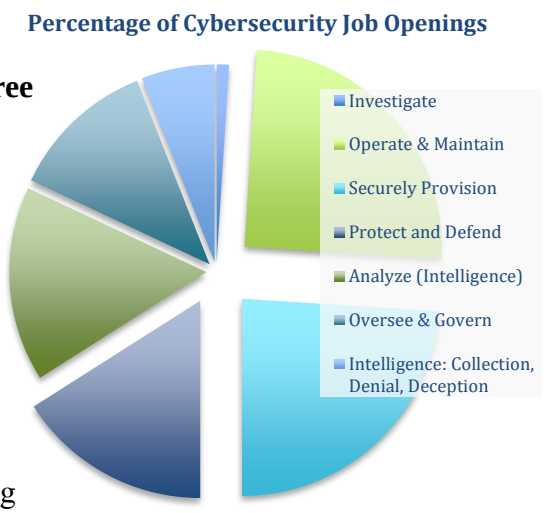
Education is a central aspect of growing a diversified economy. New digital tools, apps, and Internet resources have the potential to deliver gains to both students and teachers. Students with limited access to textbooks can now log on and learn with the world's best educational content on affordable tablets or e-books, while teachers have access to better continuing education. Although some research indicates that the education sector may not benefit as much as other sectors from ICT, investment in this area can have a disproportionate effect on the economy, as education is so vital to economies of the future. Based on some estimates, the technology-related productivity gains in Africa in the education sector could reach between $30-70 billion (McKinsey). ICT can also help address immediate issues. For example, Dakar University has helped address overcrowding by incorporating e-learning with the African Virtual University. These courses have helped the university, with 75,000 enrolled students, manage to provide college education despite a physical campus capacity designed for only 16,000. Nepal is leveraging 5G to extend Internet services to 500 rural community schools & colleges, and local schools in disconnected, remote, and rural communities. And of course, recent global experience with the COVID-19 pandemic has demonstrated the value of remote learning access.

D.6.3 Employers' Challenges

Even when organizations do recognize the value of digital skills, they often experience difficulty in recruiting and retaining the right talent. Across the board, among both industry and government, employers feel existing programs are not producing graduates with the right qualifications to meet their IT/cybersecurity needs. At the same time, employers themselves often compound the difficulty of acquiring qualified new hires by specifying criteria that do not match their actual needs. For example, most employers' ICT- and cybersecurity-related job openings require applicants to have considerable hands-on experience (3-8 years, on average) and significant education (often a four-year degree in computer science or a related discipline).

These aspirational descriptions are often the result of organizational leadership's or human resources department's unfamiliarity with the tasks IT professionals execute—they resort to high-level qualifications as a sort of hedge against the possibility that new hires will be unable to perform the work.

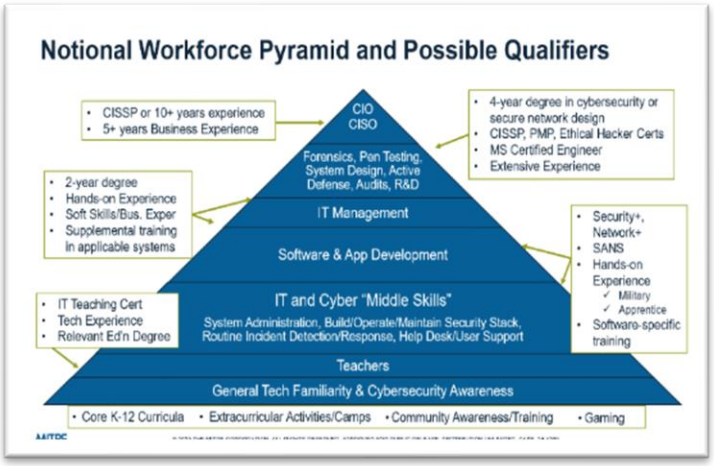
As a result, they find few qualified candidates—it is a truism that it is difficult to gain work experience when every employer requires workers to already have experience to be hired—and potential candidates who might be capable of the work are discouraged from applying because the barriers to entry are perceived to be high, in terms of both time and costly education/training. However, our research suggests that the skills actually needed by most employers—that is, the skills workers actually use in doing these jobs day-to-day—can be relatively easily and affordably attained through hands-on apprenticeships, internships, on-the-job-training, informal IT experience, and training programs focused on specific system administrator and help desk skills. Moreover, they do not typically require a demonstrated aptitude in math, science, or engineering, but rather can be acquired by most people who are comfortable with and interested in technology and the ways in which it can be used to enable different businesses and outcomes.



Our research found that while there are certainly some pockets of higher level requirements, most **employers *primarily* need workers with skills in three major NICE framework areas: Provision, Operate & Maintain, and Protect & Defend**. These are the "middle skills" (between a typical US high school diploma and a two-year degree) needed to **build and operate cybersecurity "stacks"** (networks that incorporate things like firewalls, intrusion detection/protection, and similar common features), perform **system administration** and user assistance/**help desk** tasks, and identify and **respond to incidents**. The notional job pyramid below shows the major role occupied by these "middle skills," along with similarly attainable skills in routine software development such as is used in creating websites and apps and/or adapting them to specific business processes.

Approved for Public Release Case #20-2683.

When employers—including government—frame job requirements in terms of years of experience or high-level degrees and certifications, they overlook the fact that most can be performed by people with core skills are relatively attainable, unnecessarily limiting their access to talent that might otherwise be available. This conclusion was recently validated by the Aspen Institute Cybersecurity Group, which is a leading cross-sector, public-private cybersecurity forum comprising former government officials, Capitol Hill leaders, industry executives, and respected voices from academia, journalism, and civil society. The Group, which includes AIG, Cloudflare, the Cyber Threat Alliance, Duke Energy, IronNet, Johnson & Johnson, Northrop Grumman, Symantec, Unisys, and Verizon recently focused on the need to address the cybersecurity skills gap, identifying misaligned and inconsistent job descriptions as a significant hindrance to acquiring talent. As a result, 31 major companies that participate in the group, including Apple, Facebook, Google, and IBM, recently announced they are joining together to change their cybersecurity job descriptions and requirements to attract more talent—particularly women and individuals without college degrees—to cybersecurity jobs. Specifically, the companies want to **eliminate requirements that candidates have four-year bachelor's degrees and gender-biased job descriptions in favor of skills-based descriptions**, noting that a university degree is not a good proxy for digital skills or talent.



Unfortunately, there is no common guideline to help employers—particularly those outside of the ICT sector—identify their skills-based needs, and what programs or experiences may meet those needs. More specifically, there are generally not enough accessible, affordable hands-on programs to produce the kind of experience needed by employers, despite growing need. Developing these kinds of programs offers ideal opportunities for public-private partnerships between government as a policy enabler, industry as a steady demand signal and resource pool, and academia, as providers of foundational skills at the primary and secondary school levels and more advanced skills at the academy, vocational school, and university levels. To facilitate these partnerships, stakeholders need to understand what kind of cyber skills they collectively need and how to get access to them—the NICE can provide a useful common lexicon providing standard skill/competency descriptors and tools for the creation of both job descriptions and training programs.

D.6.4 The Role of Government

While government is a significant employer of individuals with cyber-related skills, its needs and concerns in this area are largely (with the exception of some specialized jobs in law enforcement, intelligence, and the military) the same as those of other employers. Therefore, this framework focuses on the government's unique role as policy developer, convener, and a significant potential source of both incentives and barriers to cyber workforce development. In a given

ecosystem, the government is usually best positioned to integrate industry drivers, academia, cyber professionals, commercial training programs, and national security needs. Some of the key functions that government can provide in this space include:

- Broadly identify shortfalls and develop and publicize a long-range (10+ years) plan that accounts for present and anticipated economic drivers such as emerging industries
- "Educate the Market" – as described above, broaden understanding among industry leaders of the importance of cybersecurity skills to national security and economic growth across the ecosystem
- Formally establish a common lexicon, such as NICE, that can help align jobs, candidates, and education/ training programs and facilitate skills-based training and hiring, and encourage skills-based, rather than education/experience-based hiring in both government and industry to broaden access to diverse talent and expand training paths
- Convene academia, industry, and commercial training providers to develop specific skills-based standards that can guide training and education programs, help shape career paths, and assure employers of qualifications
- Provide opportunity and incentive to cooperate across government and industry in career development and retention, including at the local level
- Eliminate barriers to cooperation and investment in training, and to competitive compensation (especially in government jobs) for skilled employees
- Incentivize primary and secondary schools to include cybersecurity and technology literacy and problem solving in foundational curricula, and help develop/establish that curricula and associated extracurricular programs where appropriate
- Encourage underrepresented groups, such as women, to pursue cybersecurity careers
- Encourage the use of apprenticeships, internships, and other hands-on programs through partnerships between industry and educational institutions
- Consider creating rotational job programs and exchanges through public-private partnerships and private sector incentive programs to create a deeper cybersecurity bench across ecosystem
- Define standards for and encourage colleges and universities to pursue government grants and accreditations for cybersecurity education programs, such as a Cybersecurity Academic Center of Excellence accreditation (for schools) or Scholarship for Service programs (for students)

D.6.5 The Impact of Culture

Though MITRE's research was not specifically focused on culture, some observations related to the role of culture in fostering an effective cyber workforce development pipeline did emerge.

- Innovation/Openness to Change – communities and organizations that support trying new things or breaking out of traditional paths are more successful in conveying the value of digital skill sets and encouraging people to pursue them, including in K-12 educational curricula.

- Acceptance of Risk/Failure – communities and organizations that are more tolerant of risk—particularly social risk—and accept the possibility of temporary failure as a "cost of improving" are typically more open to the adoption of ICT, more open to pursuing emerging applications of technology and data, and more supportive of reskilling employees or training new hires in skills that are not yet central to their business.
- Strong Education Focus – The earlier youth are exposed to digital skills and their global applications, and the more easily older people are able to access information how acquiring digital skills might help their job prospects and pursue those skills, the more responsive the cyber workforce pipeline will be. Communities and organizations that strongly support education as an inherent value—particularly for girls—are typically more open to establishing career paths and training programs in digital skills, are better able to convince women and girls they are qualified for cyber-related courses and careers, and are better at devising career progression tracks with associated training that can help in both upskilling and retention.
- Tech Savvy – The rapid pace of technological (and attendant social) change is disconcerting to many. Communities and organizations that foster a familiarity and comfort with technology, even at fairly basic levels like mobile devices and applications, are more successful in instilling the interest and skills needed to pursue ICT-related jobs, even—or especially—when those jobs are outside the ICT sector.
- "Training For" vs. "Training In" – Many people are not inherently interested in ICT but are open to using it to accomplish aims in other areas such as healthcare, social work, business, marketing, or the trades. Educators who can frame digital skills in terms of their relevance to students' interests will create an environment in which it is more likely that individuals not inherently interested in computers will pursue those skills and bring them to bear in their future careers outside of ICT. Conversely, educators who can reach tech-minded students with the message that soft skills are also important can help those students become more competitive in job searches and better employees in the long run.

D.6.6 Skills Development Paths

Among the most important conclusions of MITRE's research is that there is no "best path" for acquiring cyber skills. Rather, there is an array of opportunities in any ecosystem that presents a variety of opportunities to develop partnerships and leverage local employers to focus "demand" in a way that can shape and increase availability of locally appropriate solutions.

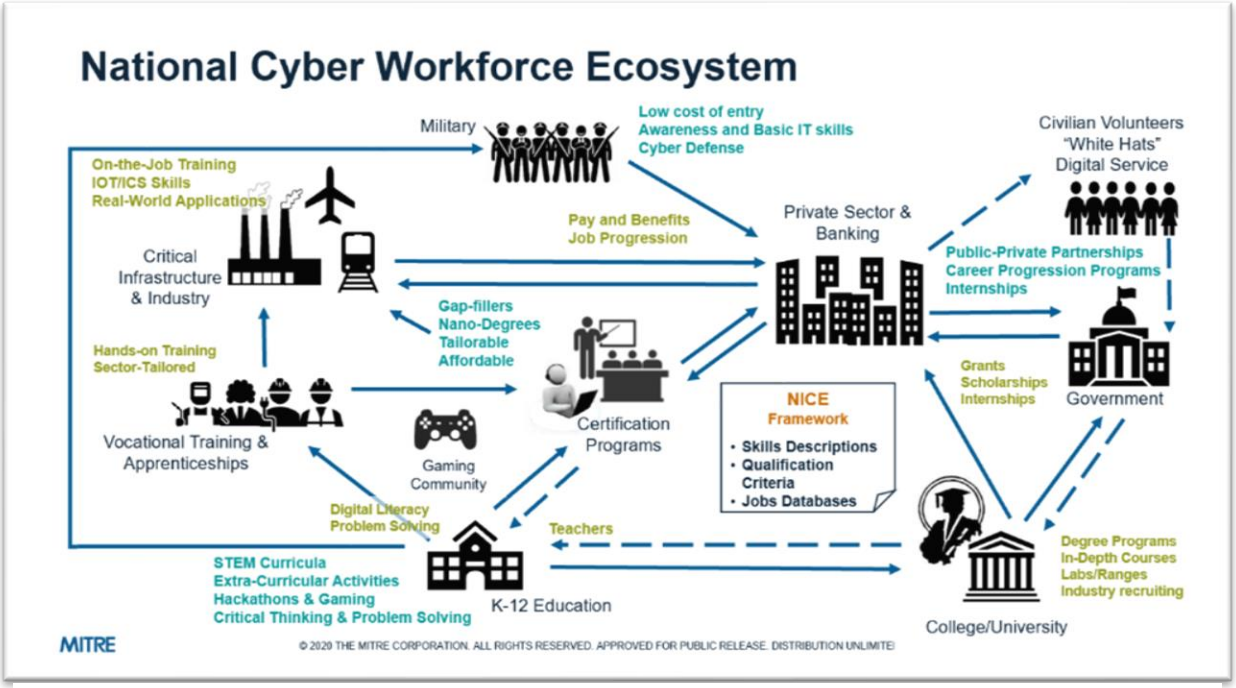


Figure 11: Notional Cyber Workforce Development Ecosystem

The graphic above depicts a notional national workforce ecosystem, but nearly all ecosystems will have several of the components represented in the picture. Each component represents an opportunity for cyber skills development, whether on the supply (academic and training institutions) or the demand side (critical infrastructure, industry, government, the private sector and banking). Some components have roles on both the demand and supply sides, through programs they provide, sponsor, incentivize, or make more accessible—government typically plays the most diverse role through policy, grants and scholarships, its own hiring needs, and its influence on academic standards and curricula. Some potential partnership opportunities suggested by this depiction are described in greater detail below. Other insights into cyber workforce development that address elements of this ecosystem include:

1) **Early education** (K-12) focus on STEM and problem-solving skills is important
   - **Cybersecurity awareness should be a fundamental skill**, taught to all students.
   - Hands-on extracurricular activities like hackathon teams, programming classes, robotics, and even gaming provide an awareness path not dependent on schools.
   - The few students who are even aware of cyber options feel they are nerdy and math-intensive—programs that demonstrate relevance to students' interests can help spark interest—especially for girls.
   - Vocational training programs that provide hands-on cybersecurity skills to middle and high school students are emerging but are still rare—such programs can access entire

categories of young workers that might otherwise never consider a cyber-related career because of perceptions that they are academically demanding.

2) **Apprenticeships, internships, and work-study programs** can offer lower cost avenues to affordable, hands-on, tailored skills acquisition, follow-on employment, career progression, and retention

3) **College and University programs** should better align with employer needs for IT operations and cybersecurity: system administrators, security stack operations, incident response, user/app support
   - Few universities offer programs that include these subjects except as tangential material to more theoretical degrees in computer science, data analysis, or network engineering.
   - Current University programs tend to limit cyber and IT-focused classes to computer-focused programs (e.g., computer science, network engineering)—including IT &
   - Cybersecurity fundamentals as core courses can help students understand these are relevant to all future careers.

4) **Certification programs** need to adapt.
   - With some exceptions, these programs are expensive and do not offer the kinds of hands-on experience trainees need in order to be qualified for most jobs. For example, the Certified Information Systems Security Professional (CISSP) certification is one much sought after by employers, but it includes little practical training—rather, it provides a broad understanding of considerations relevant to cybersecurity. As indicated on the skills pyramid above, it is more suitable for management.
   - While many certification programs claim to map to the NICE framework, the specific skills they provide are often more oriented toward familiarization than qualification.
   - To become more effective, an accreditation standard that focuses on whether a program offers sufficient hands-on training in core cybersecurity skills like access management or incident detection and response would be helpful, as would a cross-reference of what certifications provide what skills, so that non-ICT sector employers can more easily match certifications with hiring needs.

5) **Employer Training Programs**, whether offered internally (such as through on-the-job-training or apprenticeships) or through sponsored programs (such as work-study options) in local academies and colleges, can offer substantial value to both the employer and the trainee, providing a stipend during training while ensuring the acquired skills are precisely aligned to their systems and processes.

D.6.7 Realigning Incentives

Many of the shortfalls in cyber workforce development across a particular ecosystem result from a misalignment of incentives. The summations below are drawn from the findings of the Aspen Institute Cybersecurity Working Group's investigation into cyber workforce development.

D.6.7.1 Demand-Side

The complexity of employer requirements in job listings means more than 50% of applicants are considered "unqualified," particularly in cybersecurity (vs. IT) roles. Cybersecurity practitioners represent a continuum of operators, engineers, scientists, developers, defenders, investigators,

and analysts. These roles do not all require the same amount of education and training, but most employers post job qualifications as if they do—their cyber-related job descriptions are often "a full-blown recruiters' wish list" rather than an accurate description of the skills needed for a job. This long set of requirements in job postings can turn off applicants—particularly women—who may very well qualify based on the actual requirements of the role. For example:

- 84% of postings studied required a bachelor's degree—a hurdle that requires time and money many potential candidates—particularly those with family support obligations—cannot afford.
- 83% required at least three years of experience, even though many of the jobs could be characterized as entry-level or journeyman positions.
- More than 35% required certification, with the top three desired certifications requiring a minimum of five years of experience—as noted above, many of these highly desired certifications not only are expensive, but also provide few if any of the practical skills needed for most ICT-related jobs.

Establishing a commonly agreed upon lexicon of job titles, descriptions, and associated competencies defined by specific skills, and using these rather than experience or degrees/certifications as hiring criteria can help de-escalate hiring requirements and make jobs more available to candidates who do possess the necessary skills to perform required tasks.

D.6.7.2 Supply Side:

The lack of available cyber-related job candidates starts with lack of awareness.

- Only 37% of students were advised about cybersecurity as a career
- Information about the cybersecurity career path is not easily discoverable or consumable
- Potential candidates don't understand how to navigate the myriad cyber-related options or what could be possible for them (particularly those who are focused on pursuing careers in non-ITC businesses or services)

The shortage of women in the field is another significant limitation on the pool of potential job applicants. Even though women now pursue advanced education and training at rates exceeding those of men, women currently represent less than 25% of the cybersecurity workforce. According to a Hewlett Packard internal report, women are less likely to apply for these positions than men in part because women typically feel they need to meet 100% of job requirements in order to apply, whereas men apply when they only meet 60% of the requirements.

D.6.7.3 'New Collar' Recruitment and Hands-on Training

In order to better align skills requirements in hiring, some companies are reworking their internal career development paths so employees can develop skills through mentorship, apprenticeship, and on-the-job training. As one example, in response to their cyber workforce shortage, IBM has been running internal technology-focused apprenticeships for trainees they call "New Collar" employees for more than three years and has found them to be quite effective (per IBM Vice President of Compensation, Benefits & HR Business Development Joanna Daly). "We've proven that it does [work]…We're on our third cohort of cybersecurity apprentices [and] 90% have been hired in full time cybersecurity roles when they finish."

Such work-based learning programs can be the key to aligning worker and employer needs. In addition to IBM's apprenticeship model, there are options ranging from sponsored certifications to work-study partnerships with local academic institutions, as shown in the figure below.

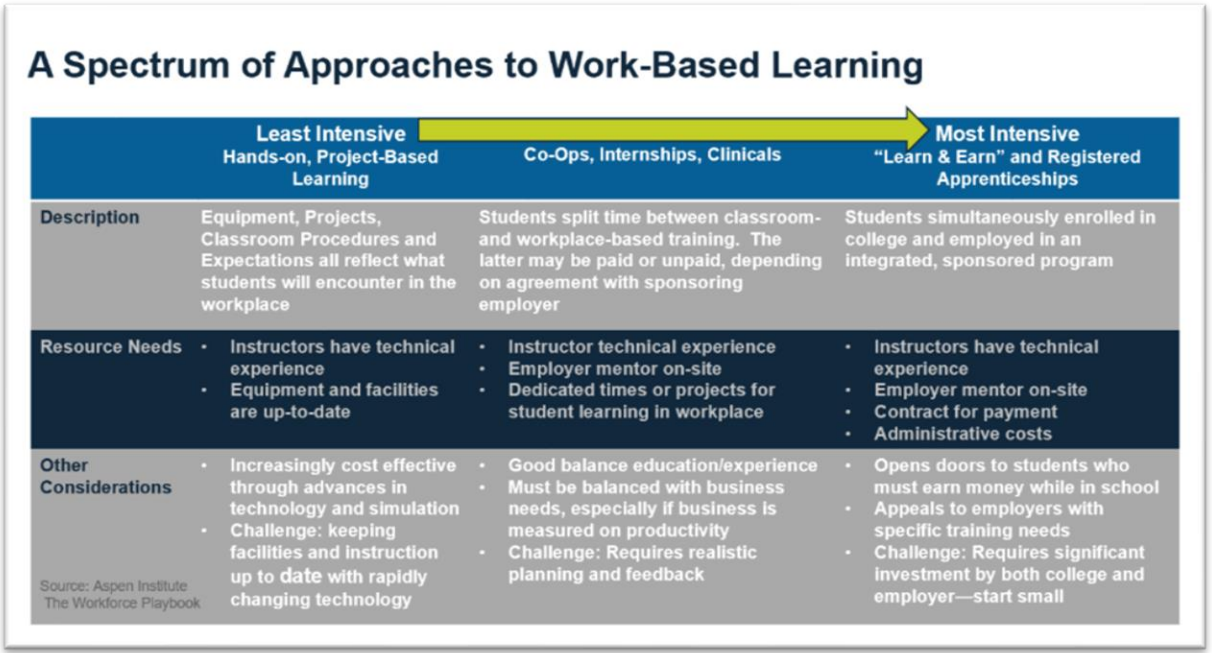


Figure 12: The Aspen Institute's Workforce Playbook summarizes various approaches to work-based learning

Some things employers can do to foster relationships with community colleges, academies, or other potential training partners include:

- Supplement Human Resources
  - Arrange for faculty to visit worksites to maintain familiarity or establish job-sharing agreements so faculty can work part-time on the same systems they will train students on.
  - Supplement salaries for faculty and program leaders.
  - Provide program supervision and faculty mentors to keep the academic program in tune with employer culture and needs
- Funding for materials, equipment, and space required for high-quality learning environments.
  - South Dakota's Mitchell Technical Institute has low-cost annual lease agreements with an equipment supplier that employs graduates of its precision agriculture program, ensuring that technology can be upgraded regularly at a cost the college can afford.
- Student Support
  - Provide industry mentorship to interested students focused on the culture, expectations, and required skills for new hires in their profession.
  - Help students afford training by providing scholarships or sponsorships, ideally including a stipend so students with financial responsibilities can meet them while receiving training.

    - North Dakota State College of Science matches employers with entering students who are interested in their industry; the businesses help fund students' textbooks and tools, and in some cases even a full ride through the program, alleviating financial stress for students while serving as an employer recruiting mechanism
- Advocacy
  - CEOs can accompany college presidents to advocate that policymakers provide funding for their colleges or modify rules that increase costs or reduce flexibility.
  - Employers can also represent the college at area recruiting events, or advocate for a bond issue needed to build and improve facilities.

D.6.8 Public-Private Partnerships (P3)

One of the most consistent themes that emerged from our research is the conclusion that no single component of the cyber workforce ecosystem can meaningfully improve the talent pipeline alone. Joint efforts among government, industry, and academia are key to establishing an effective policy environment, creating a strong demand signal, fostering effective training programs, and creating opportunities for cyber professionals to move seamlessly among government and industry employers.

D.6.8.1 Recommendations for Employer-Academia P3 Initiatives

Local solutions have proven effective in establishing programs that enhance workforce pipelines. For example, a regional approach can help multiple large employers in a single sector address significant workforce gaps, countering employers in neighboring regions who are competing for the same workers. Community colleges or similar institutions can play an important role in organizing such regional solutions. However, it is important that employers understand what it takes for colleges to build and expand programs, and for colleges to understand how to demonstrate business value to employers. Facilitators of industry-academia discussions should

Considerations for College-Employer Partnerships			
Executives	**Front-Line/Hiring Managers**	**Human Resources**	**Recent Alumni Feedback**
• To what extent do employer and college goals align? • Is the employer willing to make the investments needed to solve talent pipeline challenges	• Can the college help close skill gaps through better quality programming? • Can better training reduce time-to-competency for new hires?	• Can the college provide the quantity of talent needed? • Could the employer save money and time spent on recruitment?	• What kind of feedback to employers might be helpful (e.g., onboarding practices, new-hire management)? • How can programs better align training to real-world requirements?

act as a neutral convener, there to listen to and confirm common industry needs and discuss possible solutions without aggressively positioning a particular solution.

Figure 13: Aspen Institute Cybersecurity Working Group P3 Considerations

It is important in establishing these sectoral partnerships that the stakeholders discuss and document the roles each party will play in: delivering education in classrooms and workforce settings; securing and contributing funding needed for equipment, tuition and fees, and other costs; setting agendas, convening partners, and managing partnership activities; and collecting and reviewing data to assess progress toward common goals. To this end, they should set

appropriate goals, metrics, and responsibilities, such as pipeline targets to be filled by a specific date. Several industry-academia P3 examples demonstrate the range of possible agreements:

- IBM Cyber Day for Girls: Girls are exposed to opportunities in STEM while they learn about protecting their online identities and securing the Internet of Things. They also learn about exciting careers in cybersecurity and are introduced to female role models studying and working in the field.
- P-TECH: Pioneered by IBM, P-TECH is a public schools model spanning grades 9-14 that brings together the best elements of high school, college, and career. In six years, students graduate with a no-cost associate's degree in a technical discipline, along with the skills and knowledge they need to continue their studies or step easily into well paying, high potential 'new collar' jobs.
- University of Maryland Cyber Scholars Program: This collaborative partnership, launched and sustained through a grant from the Northrop Grumman Foundation, is preparing the next generation of cybersecurity professionals, with a focus on women and other underrepresented groups in this fast-growing field. Launched in 2013, it supports 15 – 20 scholars annually.
- GenCyber: The GenCyber program provides summer cybersecurity camps for students and teachers at the K-12 level. The goals of the program are to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation, help all students understand safe on-line behavior, and improve teaching methods for delivery of K-12 cybersecurity content.

P3 training strategies should address the needs of diverse students, as well as employer partners. One of the most important determinants of the success of a program in attracting trainees is accessibility, which requires that program providers consider:

- The time of day courses are offered (in order to support trainees' ability to learn while holding a job or parenting)
- Program costs, including fees, tools, and other expenses
- Opportunities for students to earn income while taking courses
- Program and course locations, and ease of transportation to those locations

In addition, it is important that both trainees and employers have some assurance of the quality of the program in terms of the skills it will deliver. The college should continually evaluate program quality through student performance on third-party or industry certification examinations. To ensure that programs are delivering the skills needed, employers may collaborate with educational institutions to include specific work-based learning requirements (such as internships, co-ops, clinicals, and apprenticeships) in appropriate courses—an approach that also gives them exposure to students prior to graduation, and may offer the opportunity to provide stipends that can further enhance the desirability and feasibility of the program.

Where employers rely on industry or cybersecurity certifications, a sectoral P3 training program will consider not just one credential, but the trajectory of credentials required for continued career progression in the field. At the college or university level this can be done within a constellation of programs by embedding industry-recognized certifications in bachelor's degrees, defining and awarding "nano-degrees" that represent skills acquired in individual courses or sets

of courses, and arranging courses within a curriculum to deliver skills in the order needed for a standard career progression, so that students who can only take one course at a time will nevertheless gain substantive value in the form of new skills that align with their career development with each additional course completed. Industry partners can then sponsor particular courses they require, and/or particular trainees who are ready to progress but lack specific skills. It should be noted that "soft skills"—writing, communicating effectively, managing professional relationships, organizational skills, etc.—are among the skills many employers say they find most lacking in new hires, so including some courses on professional communications, or some material within each course on writing and presentation, is likely to be a valuable program addition.

D.6.8.2 Government's Role in P3 Training Programs

In addition to the roles described in the summary of findings above, Government also has a key role in P3 aimed at improving cyber workforce development. Governments typically have access to mechanisms not available to other stakeholders, such as funding for "public good" initiatives, the ability to launch national initiatives such as apprenticeship programs, broad influence over public school curricula, and the ability to offer tax, licensing, accreditation, or other incentives to organizations that fulfill particular programmatic requirements. Some options for governments interested in supporting P3 training programs include:

- Provide grants to students pursuing cybersecurity curricula—college degrees or certifications—in return for 5 years of government service
- Work with local key industry sectors to develop notional career ladders for cybersecurity and IT personnel that recognize and support the value of gaining experience in both arenas—for instance, government service as a pre-requisite for some industry jobs, or higher pay categories for government workers with industry experience in a certain area.
- Collaborate with Universities to develop and fund programs that include appropriate certifications or hands-on training programs relevant to industry needs
- Cooperate with industry to establish training metrics, hiring fairs, and possibly lab space or other equipment to qualifying programs.
- Leverage military training to provide basic digital skills or certifications, and/or qualify individuals for scholarships and stipends if they pursue follow-on IT training and government service after completing their military commitment.
- Provide tax or other incentives to industries willing to participate in job exchanges with government organizations.
- Establish a Cyber Reserve that allows cyber professionals at the mid-point or later in their careers to qualify for (i.e., a security background investigation might be required) and participate in an "on-call" reserve to augment government cyber expertise in an emergency. Support with periodic refresher training in appropriate procedures.
- Establish public school programs specifically aimed at attracting girls into academic programs that deliver digital skills, including by incorporating those skills into course material focused on the general role of technology in non-ICT career fields as well as on cybersecurity. Include "milestone" projects designed to give girls the confidence that they do possess the aptitude to pursue jobs that require digital skills.

- Encourage young cyber professionals to pursue government positions as first jobs (recent US CIO Council initiative). Even if they move on to industry in pursuit of higher salaries after a few years, they will have acquired useful experience and contributed to a more affordable government workforce, and may choose to return to government later in their careers.

D.6.9 Using the NICE Framework in P3 for Cyber Workforce Development

This report has repeatedly mentioned the need for a common lexicon to facilitate the development of training paths that meet the needs of employers, including government. Although the NICE framework has been in existence for years, it has not yet been widely adopted, although key corporate members of the Aspen Institute Cybersecurity Working Group have recently committed to using it. One reason the framework has not enjoyed wider use is simply that most companies have "evolved" into requiring digital skills as their business processes have increasingly come to rely on ICT. As a result, their job descriptions have often been adapted from previous templates associated with related business functions. Human resources offices are often using a combination of plain language descriptions of what they understand to be the job's tasks and a "wish list" of qualifications offered by the IT experts on their staff—these may work adequately for each individual company (except for the fact that, as noted above, they are likely to considerably overstate the necessary qualifications for many jobs), but collectively this practice generates an inconsistent demand signal to training providers and job applicants, who must try to decode and compare these descriptions in order to determine what skills are most commonly required. This section addresses how government, industry, and academia can use the NICE framework to help create a stronger, more consistent, and more relevant cyber skills demand signal.

NICE was designed specifically to provide a set of standardized descriptions of cyber-related skills, work roles, and (in its most recent iteration) competencies that can provide a common language for employers, trainers, and job seekers. Ideally, government, industry, and academia representatives will use NICE to collectively develop job descriptions that reflect the needs of many hiring organizations. The following are high-level steps that can be taken toward this end.

- Within a given ecosystem (national, regional, city/local, or sectoral), Government, in its role of convener across public interests, sponsors a multi-day Digital Workforce Development conference to which it invites representatives of key ecosystem employers. The invitee list may be based on geography or industry, as appropriate (some areas have a few key industries that comprise a major share of the economy; others are comprised primarily of smaller employers across multiple sectors and services). The invitation should be preceded by a strategic messaging effort aimed at "educating the market" in order to convince non-ICT industry representatives that digital workforce development is something they should be interested in and can meaningfully contribute to. Government should plan to participate as an employer as well as convener. Attendees should have a good understanding of their IT and cyber-related jobs and the skills required to perform those, as well as an understanding of the role of ICT and data in their business.
- A facilitator should help guide the conversation with the goal of identifying and mapping those skills most needed across the entire participant group. Mapping the overlaps in the skills required shows the areas of greatest common need, such as the "middle skills"

discussed previously (areas with less concentration, such as high-end forensics skills, while still valuable, may not be initial focal areas). These should represent a significant subset of the core skills graduates and trainees will need to be successful at entry level positions in their cyber workforce ecosystem.

- Once the set of skills (which may be described generically) is identified as warranting further development, subject matter experts can use the NICE Mapping Tool (https://niccs.us-cert.gov/workforce-development/mapping-tool) to develop standardized skills and work roles/competencies descriptions. Ideally, all participants will agree to transition their IT and cybersecurity related job descriptions to language that reflects these agreed-upon standardized descriptions, with the understanding that a certain amount of tailoring may be required.

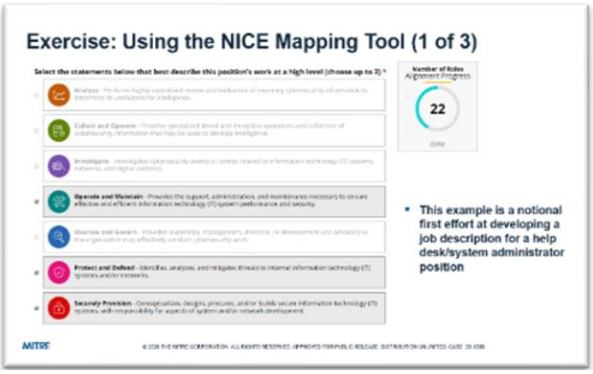


Figure 14: The NICE Mapping Tool can be used to create standardized job descriptions

- Universities and other education and training/certification programs can then develop curricula and certifications that deliver those skills—increasing the incentives to industry and government to support those programs.
- Industry and government can consult to identify areas where training in one area can benefit another, and develop partnerships and incentives such as reciprocal hiring, overlapping career paths (that reward experience in both arenas), internship and exchange programs, continuing education fellowships, "cyber reserve" programs, etc.
- Youth development is also important! Many skills can be incorporated into primary and secondary school curricula to increase the number of young people with interest in pursuing careers that require or are enhanced by digital skills. Ideally, most young people must emerge from primary school with the skills and interest to pursue technical training that will be of use to virtually every employer in the economy, and will also prepare them for a possible future in which remote work or telework is common and expected.

D.7 Cyber Workforce Development: "How Might We…"

Like the broader CSDI Framework, this framework emphasizes Design Thinking approaches to innovative solution development. A key tool in the Design Thinking toolkit for ideation is the "How Might We…" exercise in which participants brainstorm creative approaches to meeting identified needs. In that spirit, the following ideas are offered as food for thought in developing cyber workforce development solutions that fit the needs of a particular ecosystem or organization.

D.7.1 …Grow Tech Interest in K-12?

- Develop and adopt Science, Technology, Engineering, the Arts, and Mathematics (STEAM) programs for K-12 education that incorporate both technology and problem solving/soft skills across curricula. Example: a once yearly cross-subject block that incorporates a science fiction book (language arts) with social and historical (social studies) themes, and corresponding blocks exploring the technical (Math and Science) concepts described by the author.
- Offer digital technology blocks in K-12, focused on interesting challenges like basic robotics in elementary school, simple game development in middle school, or mobile app development in high school that addresses problems students and/or industry sponsors care about. Emphasize security considerations and include design and marketing aspects to familiarize less technically minded students.
- Fund and staff extracurricular activities such as hackathons, robotics, or programming classes; digital 'capture the flag' competitions; or summer camps, and the inclusion of technology and cybersecurity considerations in other programs like Young Entrepreneurs and Future Farmers.
- Leverage the Gaming culture and community with sponsored cyber security-focused contests like capture the flag, system penetration challenges, etc.
- Actively include girls and other underrepresented groups by allowing students to pick problems to which they could apply technology, such as climate change, animal protection, or social media marketing – "de-nerdify" tech.
- Teacher Training! Help teachers better understand how they can introduce technology concepts, and where to find supporting resources.

D.7.2 …Better Align Degree Programs with Industry Needs?

- Increase focus on Community Colleges and "Academies" or vocational schools as sources of valuable training, and incentivize them to develop, accredit, and provide certifications in cyber-related offerings.
- Re-focus University and Community College degree programs and tech-related survey classes on cybersecurity rather than computer science and network engineering.
- Normalize an emphasis on the role of cyber and cybersecurity in every field of study, and in core graduation requirements (e.g., Tech Concepts 101).
- Partner with Industry to identify local employment opportunities, recruit students, and sponsor tailored training programs (including labs or other hands-on support) to develop appropriate skills.
- Integrate 2-year programs with professional certifications relevant to industry hiring needs.
- Offer accredited "nano-degrees" (hyper-specific learning programs, usually offering certifications).
- Partner with Udacity, Coursera, or similar nano-degree institutions in which students spend 10-15 hours a week in short but challenging, university-comparable courses, each culminating in a specific certification.

- Work with industry to define and create a 'constellation' of nanodegrees focused specifically on employer needs for post-secondary students, rather than or in addition to a bachelor's or associate's degrees. Nanodegrees are typically cheaper than 2-year colleges, and much cheaper/more focused than University degrees.
- Make training affordable/attractive through scholarships focused on pursuing cybersecurity-related skills (ROTC model)

D.7.3 …Incorporate Non-traditional Training Approaches?

- Develop standardized, accredited on-line/virtual training, including complex capabilities like AWS learning environments and cyber-ranges, and make available through community colleges or similar institutions.
- Sponsor 'qualification events' (hackathons, bug-bounties, contests) tied to internships/ scholarships.
- Combine Gaming culture with a "$100 Laptop" program—pre-load laptops with bootstrap learning games (Intelligent Tutoring Systems) focused on cyber concepts.
- Leverage military skills/training through Veteran transition programs focused on IT and cybersecurity "Middle Skills" (US Army already sponsors a 6-month transition program).
- Incentivize apprenticeships/work-study programs for "New Collar" and re-skilling trainees.
- Employ Mobile Training Trucks to bring hands-on training labs to schools and organizations.
- Provide customized and (if necessary) translated Khan Academy video tutorials on STEM subjects to selected schools and train teachers on their use.
- Let citizens self-select into training programs. Start with cyber readiness assessments, potentially through mobile games or applications ('The Last Starfighter' model). With an effectively marketed program there could be a "prestige" effect to participation.
- Establish and facilitate access to standardized aptitude testing (available to youth and adults) that can qualify candidates for free or reduced cost training in cybersecurity and related skills. The FBI has reportedly had some success with personality attribute screening—this could be one component. Consideration should be given to how to support recruits during schooling (for instance, through a ROTC- or AMERI-CORPS-like service-for-schooling program).
- Use local colleges/universities, community centers, churches, etc. to host seminars on cyber-related topics, with opportunities to gain training opportunity information.
- Investigate Intelligent Tutoring Systems (ITSs)* (The 'Diamond Age' model). Research suggests ITSs at the secondary school level are more effective than teacher-led, large group instruction; non-ITS assisted instruction; or textbooks/ workbooks, and just as effective as competent individualized or small-group instruction. This approach could provide access to quality education at disadvantaged schools, and be used as whole-class, small group or one-to-one approach with teachers as guide/facilitator. This idea requires careful attention to learning goals, design, and integration.

D.8 Cyber Workforce Development Initiatives

This section briefly introduces a number of existing cyber workforce development programs in the US and around the world. The diversity of these case studies is indicative of the opportunities to develop innovative P3 approaches that reflect the specific needs of a particular country, region, or employer.

D.8.1 US Examples

- California's CyberHub seeks to organize partnerships between educators, public, and private institutions to encourage **research and innovation in cyber education** among high school students.
- Cisco, Microsoft, Amazon, and others have established a public/private partnership to **'train the trainers'** (K-12 and post-secondary teachers) in cybersecurity and computer science (including providing paths toward technical training/certifications), and offer on-line training for HS students on cyber topics.
- Glitch Game Testers was a 3-year partnership between Georgia Tech and Morehouse University to **encourage more African American high school upperclassmen to pursue computer science**. Students work as paid videogame testers while taking workshops in computer science—more than half of participants continued to computing careers.
- IBM's **"Learn and Earn" Apprenticeship** program combines on-the-job training with job-related structured education and/or hands-on instruction. It was founded on the idea that apprenticeships are a proven model in the skilled trades that is seeing significant growth and adoption across the tech industry today. Highly scalable, this model provides opportunities to hire talent eager to learn, and for employers to train them in the exact way needed for their open roles while paying the trainees a graduated wage as they progress in skill—earning loyalty while cutting costs.
- The Michigan Department of Education runs **grant programs** to encourage initiatives aimed at 1) creating a STEM culture; 2) empowering STEM teachers; 3) integrating business and education; and 4) ensuring high-quality STEM experiences. Grants are approved when proposals support programs in robotics, computer science/coding, and engineering
- Merit (a non-profit) partners with Michigan universities to develop and offer bachelor's and master's degrees in Cybersecurity; Information Systems; Information Assurance; and Intelligence Analysis; and to **prepare cybersecurity professionals for certification exams** (CISSO, CDFE, CPEH, CPTE)
- Monumental Sports & Entertainment (MSE) partnered with Deloitte to **promote STEM education** for youth of all ages in Washington D.C.'s Ward 8, home of the Entertainment and Sports Arena. Together they presented "De-Mystifying STEM" at a Washington Mystics home game, showcasing the science, technology, engineering and math principles that power the game of basketball.
- The North Dakota State College of Science (NDSCS) is a community STEM-focused college whose president visits all 42 high schools in the southeast region of North Dakota

to engage K-12 educators on STEM issues. The college also conducts a residential summer program for **high school counselors and educators** that helps them see community college programs as "real" college options and builds understanding of how today's technical jobs differ from those of the past.

- The Northern Virginia Community College (NoVa) **Associate of Applied Science (AAS) degree in Cybersecurity** is designed for both "re-skillers" with degrees in other disciplines and new students. Program skills are aligned with the NICE Workforce Framework 2.0 and the National Security Agency/Department of Homeland Security criteria for Cyber Defense Centers of Academic Excellence (CAEs)
- At Northeast Wisconsin Technical College, the business and information technology division created a learning map detailing not just the courses students must take, but key **career planning, preparation, and experience milestones** that students should achieve by specific points during the two-year program.

D.8.2 International Examples

- **Indonesia's Accelerated Work Achievement and Readiness for Employment (AWARE) program** aims to build a future-ready workforce. The first project was a joint initiative between the Education Development Center (EDC)—a non-profit—and the JP Morgan Chase Foundation. AWARE creates direct links between students, schools, and industry leaders to **support work-readiness among youth through structured, work-based learning in collaboration with over 65 private sector companies**, including BMW, Globe Telecom, LG Electronics, and Schneider Electric. The program leverages the EDC's Work Ready Now! curriculum to deliver work readiness preparation, including interpersonal communication; innovation challenges to address community and business challenges; and projects where students design and build their own businesses. The first AWARE program trained 4,347 students, of whom 98% were placed in structured, on-the-job training--nearly half of that cohort is already employed. In its first year of operation, AWARE2 (a follow-on effort focused on the ICT sector) **trained more than 90 teachers and 2,000 students and engaged over 100 firms in work-based learning** programs. AWARE has trained over 200 ministry officials on their approach, and the Indonesian Chamber of Commerce and Industry is exploring expanding the AWARE approach to all its members.
- **Generation Kenya** and **Get Smarter** are non-profit programs founded by McKinsey in partnership with USAID and focused on developing skills among Kenyan youth. Under these programs, 180 local employer partners operate 37 training locations, each offering 6-8-week **"boot camps" focused on technical and "soft" skills** needed for retail and financial sales, customer service, and apparel manufacturing. More than 8,000 youth had been trained by 2017.
- **Kabakoo**—which means "to wonder" in the Bamanan language in West Africa—is a pan-African network of schools that aims to empower young Africans with innovation skills. It has expanded to three campuses in Bamako and **trained nearly 500 middle school, high school and university students in rapid prototyping, robotics, web design and biotech** since 2018.

- **Mexico** is building a cyber workforce ecosystem starting with its top universities, which reportedly **graduate over 120,000 new engineers a year** (more than the US). There are 16 technology institutes and 12 universities graduating more than 8,000 technical and engineering students every year in Jalisco alone. In addition, the Mexican government has instituted programs like Reto Zapopan to keep talent local, and the nonprofit startup GDL is helping **attract Silicon Valley startups and global ICT companies** including Toshiba, IBM, Oracle, Cisco, and Intel to Guadalajara.
- Around 1.7 billion women in low- and middle-income countries do not own mobile phones, and the gap in Internet usage between men and women has grown in recent years, with significant implications for national economies. In 2018, **USAID** launched the **Women Connect Challenge** to improve **women's and girls' access to, and use of, digital technologies.**
- **Vietnam's TEKY STEAM** supports children ages 6–18, with 16 labs in 5 cities, and 30 partner schools across the country delivering 9–18 month-long technology courses. It is **focused on teaching technology skills** through modules on programming, robotics, website design, multimedia communications and animation--students spend about 80% of their learning time interacting with technology. TEKY also hosts an annual Minecraft Hackathon for over 1,000 students, plus one internal technology contest quarterly, as well as a holiday period coding camp and an **e-learning platform to deliver programs to students in more remote provinces**. They collaborate with several education technology partners, including Sigong Media, MIT for Scratch, Tynker, LEGO Education, RoboRobo and Maker Empire to develop tailored programming. Most recently, TEKY collaborated with MasterMind Crate to launch the Tekid-preneur program, designed to guide students in building and designing their own e-commerce websites, and launched Viet Nam's first virtual reality course for students ages 13–18.

D.9 Conclusion: Applying the Cyber Workforce Development Framework

The goal of this framework is to help teams in government, industry, academia, and the civil sector better understand the factors that affect cyber workforce development and develop innovative, context-appropriate solutions—particularly focused on hands-on "middle skills" training and public private partnerships. It was developed in response to a near universal need among our sponsor and partner organizations to increase their ability to develop, recruit, train, and retain digitally skilled workers that can fulfill the ICT and cybersecurity roles proliferating across every sector, in nearly every economy. The overriding conclusion of our research is that no one component of a cyber workforce ecosystem can bring about the necessary changes alone. Because of the overlapping and sometimes competing workforce needs of government and industry, the influence of policy and education on career readiness and retention, and the less defined role of commercial certification training providers, it is essential that stakeholders in government, industry, and academia work together to establish a consistent and relevant demand signal; create appropriate, accessible, and high quality training paths; and establish ways to enhance, rather than undermine, each other's access to digitally skilled talent in support of mutual benefits in national and economic security and citizen prosperity.

This paper describes our findings and conclusions in the areas of traditional and non-traditional education and training programs, employer considerations, the role of government, and the

impact of culture. It outlines first steps in creating a public-private partnership effort toward growing a local, sectoral, or national cyber workforce, along with P3 considerations, examples of successful programs, and a variety of "How Might We…?" ideas targeting different components of the cyber ecosystem. In addition, it is hoped interested readers will carefully consider the notional cyber workforce ecosystem graphic as a focal point for identifying potential partners and leverage points appropriate to their unique circumstances. The MITRE team that developed this framework is happy to answer any questions, provide further insight into its conclusions, discuss implications for particular problem sets, and help strategy teams facilitate their own engagements toward establishing a common lexicon and needs assessment, and developing approaches that will be effective in helping develop their cyber workforce capacity.

D.10 Cyber Workforce Development Framework References

Andres, A., Amavilah, V., Asongu, S., *Linkages Between Formal Institutions, ICT Adoption, and Inclusive Human Development in Sub-Saharan Africa. Catalyzing Development through ICT Adoption*, online at: https://rd.springer.com/chapter/10.1007/978-3-319-56523-1_10

Asian Development Bank, "Innovative Strategies for Accelerated Human Resource Development in South Asia," 2017. Online at: file:///C:/Users/cawright/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/TLWXTJT1/ict-education-sa%20(003).pdf

Asongu, S. and LeRoux, S. May 2017. *Enhancing ICT for inclusive human development in Sub-Saharan Africa. Technological Forecasting and Social Change*. Vol 115, 44-54. http://ac.els-cdn.com/S0040162517301439/1-s2.0-S0040162517301439-main.pdf?_tid=38177d9a-7e1d-11e7-a651-00000aab0f01&acdnat=1502405142_3f0a4463be95a7aca5e6dbd2e5b62077

Aspen Institute, "The Workforce Playbook," online at: https://highered.aspeninstitute.org/wp-content/uploads/2019/06/The-Workforce-Playbook_Final.pdf

Aspen Institute, Aspen Cyber Security Group. "Principles for Growing and Sustaining the Nation's Cyber Security Workforce," online at: https://assets.aspeninstitute.org/content/uploads/2018/11/Aspen-Cybersecurity-Group-Principles-for-Growing-and-Sustaining-the-Nations-Cybersecurity-Workforce-1.pdf?_ga=2.172790950.42777080.1582944788-1976005358.1582944788

Australian Cyber Security Growth Network, "Australia's Cyber Security Sector Competitiveness Plan: 2019 Update," Government of Australia, 2019.

Ben Kisner, "Army Deploys Videogames to Reach Recruits Amid Pandemic," *The Wall Street Journal* Online, May 17, 2020. https://www.wsj.com/articles/army-deploys-videogames-to-reach-recruits-amid-pandemic-11589734800?mod=hp_listb_pos3

Dalberg. April 2013. *Impact of the Internet on Africa.* http://www.impactoftheinternet.com/pdf/Dalberg_Impact_of_Internet_Africa_Full_Report_April2013_vENG_Final.pdf.

Deloitte, "Smart Factories," Dupress.deloitte.com/smart-factory

Digital Nepal Framework, 2019, online at: https://mocit.gov.np/application/resources/admin/uploads/source/EConsultation/EN%20Digital%20Nepal%20Framework%20V8.4%2015%20July%20%202019.pdf

Farid, Sally, "The Role of Technology to Achieve Sustainable Economic Development in Africa," Global Journal of Business and Social Science Review Vol. 4(2), 2016. pp. 30-41.

Frost & Sullivan, Executive Report, "2017 Global Information Security Workforce Study," $(ISC)^2$, Center for Cyber Safety & Education, online at: https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

Gartner, "Adopt a Lean Digital Security Organization to Mitigate the Skills Shortage (Excerpt: "Beat the Cybersecurity Skills Shortage)." Excerpt by Rob van der Meulen), August 8, 2018. https://www.gartner.com/document/3838863

Government of Switzerland, "Earn While You Learn: Switzerland's Vocational and Professional Education and Training System - A Model for Apprenticeships in the United States," Swiss Federal Department of Economic Affairs, Education and Research, 2019.

Greater Washington Partnership, "Partnering to Strengthen Tech Talent in the National Capitol Region," December, 2017.

GSM Association. 2016. *The Mobile Economy: Africa 2016.* www.gsmaintelligence.com/research/?file=3bc21ea879a5b217b64d62fa24c55bdf&download.

Harvard Business Review, "Africa: A Crucible for Creativity," Nov-Dec 2018

International Education News, "10 Surprises in the High-Performing Estonian Education System," August 2, 2017.

ISC^2 "Cybersecurity Workforce Study, 2019: Strategies for Building and Sustaining Strong Cybersecurity Teams."

Joint Cybersecurity Task Force on Cybersecurity Education Report, "Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," Computing Curricula Series, June 2017.

Laura Bate, "Cybersecurity Workforce Development: A Primer," New America, November 2018. Online at: newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/

McKinsey Center for Government, "Education to Employment: Designing a System That Works," https://mckinseyonsociety.com/education-to-employment

McKinsey Global Institute, *Lions go digital: The Internet's Transformative Potential in Africa,* November 2013, online at: http://www.mckinsey.com/industries/high-tech/our-insights/lions-go-digital-the-internets-transformative-potential-in-africa.

Michigan Cyber Academy website, http://www.michigancyberacademy.com/faq.html

Michigan STEM Advisory Council, "MiSTEM Advisory Council Grant Technical Assistance Presentation," Michigan Initiative for Cyber Education portal, online at: https://www.micek12.com/ , December 16, 2019.

Microsoft, "Microsoft Launches Initiative to Help 25 Million People Worldwide Acquire the Digital Skills Needed in a COVID-19 Economy," Brad Smith (Microsoft President) Blog, June 30, 2020, online at: https://blogs.microsoft.com/blog/2020/06/30/microsoft-launches-initiative-to-help-25-million-people-worldwide-acquire-the-digital-skills-needed-in-a-covid-19-economy/

MIT Technology Review, "A Cyber Skills Shortage Means Students are Being Recruited to Fight Off Hacker," by Erin Winick, October 2018, online at: https://www.technologyreview.com/s/612309/a-cyber-skills-shortage-means-students-are-being-recruited-to-fight-off-hackers/

New America, Cybersecurity Workforce Development Primer 2018.

NICE Framework, https://niccs.us-cert.gov/workforce-development/mapping-tool

NICERC Cyber Discovery Website, DHS Cyber Innovation Center, https://nicerc.org/events/cyber-discovery/

Palvia, P., Baqir, N., & Nemati, H. ICT For Socio-economic Development: A Citizen's Perspective. *Information & Management*.

Peter, A. S. "Cyber Resilience Preparedness of Africa's Top-12 Emerging Economies," *International Journal of Critical Infrastructure Protection*, 2017.

Philip Casesa (CISSP, PMP), "The Essential Guide to Cyber Workforce Development," Focal Point: Data Risk, July 2019.

RAND Europe (Jacopo Belasio *et* al), "Developing Cybersecurity Capacity: A Proof-of-Concept Implementation Guide," RR2072, RAND Corp. 2018.

Qiang, C., Keuk, S., Dymond, A. and Esselaar, D. December 2011. *Mobile Applications for Agriculture and Rural Development.* ICT Sector Unit, World Bank. http://siteresources.worldbank.org/Informationandcommunicationandtechnologies/Resources/MobileApplications_for_ARD.pdf

Serianu. *Nigeria: Cyber Security Report 2016.* http://www.serianu.com/downloads/NigeriaCyberSecurityReport2016.pdf

Steve Morgan, "Cyber Security Talent Crunch to Create 3.5 Million Unfilled Jobs Globally by 2021," *Cybercrime Magazine*, Cyber Security Ventures, Sausalito CA, October 24, 2019, online at: https://cybersecurityventures.com/jobs/

World Economic Forum, "There is a Vast and Untapped Pool of Cyber Talent Hiding in Non-IT Degrees." Article by Kathy Liu, May 18, 2020, online at: https://www.weforum.org/agenda/2020/05/untapped-cyber-talent-it/