PERSPECTIVES ON LAUNCHING A CYBERSECURITY INITIATIVE

By Starnes Walker and Babatunde Ogunnaike, University of Delaware

The entire concept of cybersecurity arises because of computers and how they are networked to facilitate effective operability of modern society across every spectrum of our lives.

Virtually every aspect of modern life is dependent on computers – personal, embedded, and networked; distributed, mobile, and desktop – and with the advent of the "Internet-of-Things", vulnerabilities will increase exponentially.

Cyber attacks are inevitable and constantly evolving, with ever-increasing potential for catastrophic consequences, and they are driven by a wide variety of motives including politics, espionage, crime, terrorism, and financial gain.

"Today's cyber threat is a very real and persistent one," says Peter Ware, director of The SWIFT Institute, which was founded in 2012 to extend understanding of current practice and future needs in global financial services. "Cyber-attacks are growing ever more sophisticated, and the landscape is becoming increasingly complex. As cyber criminals become better organised and funded, the way in which we protect ourselves must also continue to evolve."

In the U.S., the National Academy of Engineering has identified the establishment of a secure cyberspace as one of the grand challenges of the twenty-first century, and President Obama has recognised cybersecurity as one of the world's most serious economic and national security challenges.

And it is one that we are not adequately prepared to meet.

We have to strengthen public-private-academic partnerships if we are to find effective solutions that ensure global security and prosperity.

We need to invest in cutting-edge research to spur the innovation and discovery required to meet the digital challenges of our time, of which cybersecurity is arguably the most pressing.

And we must promote cybersecurity awareness and digital literacy, from our classrooms to our boardrooms.

In 2014, the University of Delaware Cybersecurity Initiative was launched, with the mission to be an international leader in cybersecurity research and development, education, and workforce training.

To optimise our chances of success, we have established a strategically aligned team, with a board of directors representing the entire cross-section of critical sectors, and we have launched partnerships with academic, industrial, and government organisations that have complementary expertise. No single organisation has all of the skillsets to address a challenge of this magnitude, but our combined resources will enable us to do more than any of us can do alone.

We have crafted a unique program predicated on a holistic understanding of the core fundamentals of modern cyber-technology, their ubiquitous 21st century applications, and the inherent and evolving security challenges they pose.

Through our strategic partnerships, we are implementing a multi-pronged systems approach to developing effective solutions with appropriate technological, political, sociological, ethical, and policy components.

HOLISTIC APPROACH

We believe that a holistic and systematic approach is essential for a cybersecurity program to have a lasting positive impact on society. Such an approach must include strategic organisation of the basic components of the cyber-landscape and appropriate alignment of programmatic activities with these components. In addition, potential areas of study and applications arising from that organisation and alignment must be systematically elucidated, so that multidisciplinary teams can be deployed to address identified problems.

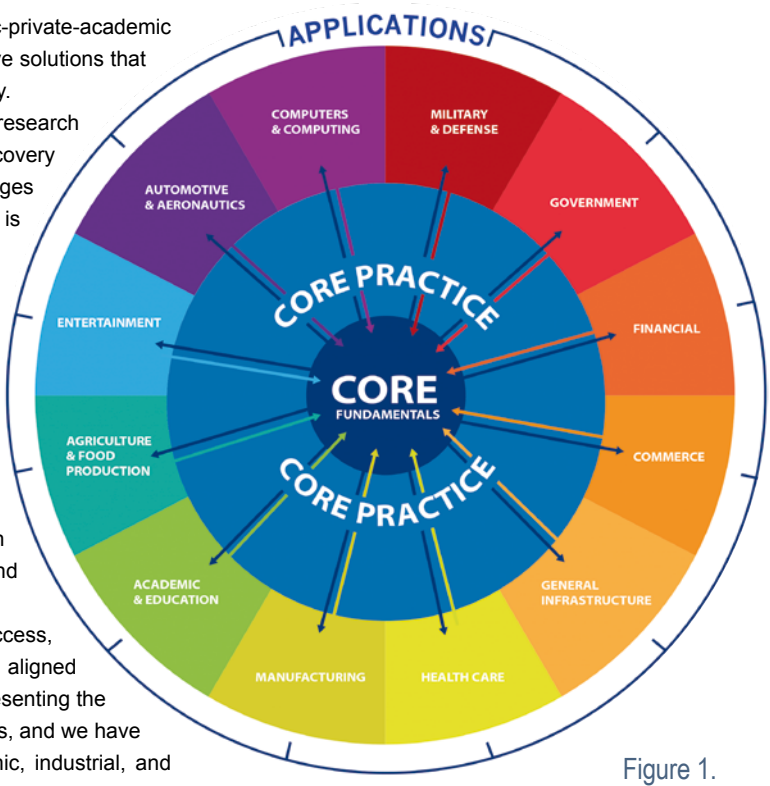

Figure 1.

Our canonical organisation of the cyber-landscape components (Figure 1) meets these criteria, providing a universal view that is independent of specific applications, industries, and fields.

At its centre are **Core Fundamentals**, or the elements upon which cyber systems are built. These elements – which include hardware, architecture, networks, platforms, software, software engineering, systems, algorithms, and computing theory – constitute the core of what enables a wide variety of computer applications. All applications, regardless of complexity and importance, have these elements in common.

The second component, **Core Practice**, comprises the work of the typical IT department of every organisation: hardware and software selection and installation, application designs, networking, systems integration, systems management, troubleshooting, and so on. All application industries and categories, regardless of specific activities, rely on such practitioners for the implementation, operation, and support of their respective systems.

Finally, **Applications** include all of the disciplines and industries that use computing for daily functions. These cover virtually every aspect of modern life, from healthcare, manufacturing, entertainment, and food production to defense, financial markets, commerce, and civil infrastructure. It would be easy, but ultimately ineffective, to focus only on these application areas; they exist on the outer ring in our organisational scheme because the work done in the core areas of fundamentals and practice is valuable across applications.

> ... UNBIASED UNIVERSITY-LED RESEARCH IS ESSENTIAL TO SOLVING THE PROBLEMS CHALLENGING THESE INTERCONNECTED COMPANIES, AGENCIES, AND INSTITUTIONS ...

This does not mean that we are going to try to cover the entire application domain; rather, we will focus on a few key applications that are particularly relevant to the state of Delaware and that reflect our current expertise – for example, financial services, manufacturing, and defence. Our activities will be informed by the applications on which we choose to focus, but by no means will they will constitute the entirety of our portfolio, and we will look to our partners to broaden the work beyond our specific areas of expertise.

RESEARCH AND DEVELOPMENT

With cyber-security affecting all of America's industrial sectors, unbiased university-led research that can be implemented across those sectors is essential to solving the problems challenging these interconnected companies, agencies, and institutions.

In our organisation of the cyber-landscape components, research and development efforts are mapped onto Core Fundamentals, with the understanding that findings and breakthroughs will be of value to all application sectors.

For example, the development of a novel "cyber-immunity" chip to be installed in computers to prevent certain categories of cyber attacks will arise from work in Core Fundamentals. Efforts in this area are motivated in part by information from Applications directly or through Core Practice. Research and development solutions are implemented in Applications through Core Practice.

Core Fundamentals research activities are conducted via a multi-pronged approach where the technical activities are carried out in collaboration with multidisciplinary teams to ensure that problem formulation and solution incorporate political, sociological, ethical, and policy perspectives as appropriate.

Over time, it is expected that activities in this area will lead to novel interdisciplinary areas of study such as cyber-epidemiology (i.e., the acquisition, curation and strategic analysis of failed and successful cyber attacks), cyber-immunology, public cyber health, sociological cyber-forensics, cyber-economics, and cyber risk assessment and management.

EDUCATION AND TRAINING

The cybersecurity workforce of 2015 is woefully inadequate.

It is not only essential that we create a pipeline of graduates skilled in the latest theories and tools required to address cyber-security problems, but also critical that we reach America's existing workforce and give everyone from entry-level workers to executives and board members the tools and training to protect the companies or organisations in which they work from attacks.

Our entire workforce is operating in a globally connected world, and we need to be smart about how we conduct our lives electronically. Knowledge of cybersecurity is not just for people who are interested in science and engineering – it is a life skill.

Education activities are primarily mapped onto Core Practice in areas such as secure software systems and analytics, secure business systems, cyber financial sector, and cyber social science. However, education activities may also be specialised for specific Applications. For example, certain academic programs may be aimed specifically at developing a well-equipped workforce for the financial sector.

Applications and Core Practice guide and inform course and curricular development, and in time, R&D results from Core Fundamentals will filter into such education curricula, either in enhancing existing courses and degrees or in creating new ones.

Training programs are primarily mapped onto Applications and Core Practice. Examples include training of current practitioners to remain up-to-date; creating certification programs for specific practice sectors and re-certification programs to keep certification up-to-date; and providing convenient "on ramp" retraining of people with no technical background to work in specific Application sectors.

With this organisation as a framework, research programs can be launched, results can be disseminated through relevant media, new products can be developed, courses can be designed, and curricula can be developed.

As President Obama said at the White House Summit on Cybersecurity and Consumer Protection earlier this year, "Our connectivity brings extraordinary benefits to our daily lives, but it also brings risks."

These risks cross the globe, and no one is fully prepared to mitigate them so that we can continue to reap the benefits of connectivity. As The SWIFT Institute's Ware points out, cyber-attacks do not discriminate.

"Regardless of where you are in the world, regardless of what your line of business is, we are all at risk," he says. "Cyber-attacks do not respect international boundaries. This means we have to work together, at a country level and an industry level."

Vulnerabilities often occur at the seams between organisations, while discovery usually happens at the interfaces. We have to work collaboratively, and to do this effectively, we need a strong set of guiding principles for all of our efforts. We believe that our canonical organisation of the cyber-landscape components is a good starting point that can work across institutional and national boundaries. ■

ABOUT THE AUTHORS

Starnes Walker is a leading national expert in cybersecurity, founding director of the Cybersecurity Initiative and Professor-Electrical & Computer Engineering at the University of Delaware.

Babatunde Ogunnaike is the William L. Friend Chaired Professor of Chemical Engineering, and Dean of the College of Engineering at the University of Delaware.