JOURNAL OF INFORMATION WARFARE

Volume 17 Issue 1 Winter 2018

Volume 17, Issue 1 • Winter 2018

ISSN 1445-3312 (Print)

ISSN 1445-3347 (Online)

Journal of Information Warfare

These attacks can range from
service to the deliberate withholding of data
Disrupt of destroy data: this is similar to the
above, but disruption can be caused to the
system collecting and storing the data, or to
that part of the system, which disseminates
Destruction of the data can occur by physical
destruction of the storage medium, or the
data itself, so it becomes irrecoverable
needed to make it useful

Journal of Information Warfare

Volume 17, Issue 1
Winter 2018

Contents

From the Editor i
L Armistead

Authors ii

Operating in the Dark: Cyber Decision-Making from First Principles 1
SL Russell, SC Jackson

Strategic-Intelligence Analysis: Contributions from an Operational-Design Orientation 16
G Duczynski, C Knight

A Taxonomy of Norms in Cyberconflict for Government Policymakers 31
NC Rowe

Towards a Reconceptualisation of Cyber Risk: An Empirical and Ontological Study 49
A Oltramari, A Kott

Uncertain Security Community: Building Western Cyber-Security Order 74
A Tumkevič

Cyber Apprenticeship: A Traditional Solution to a Vexing New Problem 87
EL Armistead, RC Guess, SR Blevins

Cyber Security in the Context of Armenia-NATO Cooperation 99
RG Elamiryan, MG Margaryan

Authors

Dr. Edwin L. Armistead is the President of Peregrine Technical Solutions, a certified 8(a) small business that specializes in cyber security, and the Chief Editor of the *Journal of Information Warfare*. He graduated from the U.S. Naval Academy (1984), earned a master's degree in Military History from Old Dominion University (1993), and a doctorate in Computer and Information Science from Edith Cowan University (2009). His major field of study is cyber power. He has published three books—all of which focus on the full spectrum of information warfare. He founded the International Conference on Cyber Warfare and Security, and the Vice-Chair Working Group 9.10–ICT Uses in Peace and War. He is a retired Naval officer.

Shannon R. Blevins is the Associate Vice Chancellor for Economic Development and Engagement at The University of Virginia's College at Wise, where she leads the college's economic outreach efforts. She works to create opportunities for government, non-profit organisations, businesses, and higher education to work together to further the progress of the region. She earned a master's degree in Business Management and Organizational Development from Averett University, and a bachelor's degree in Business and Public Administration from UVa-Wise. She has completed a certificate in Leadership Development through Darden Executive Education as well as the Management Leadership Program through Harvard's Graduate School of Education. Most recently, she, along with fellow Appalachian Prosperity Project leaders, facilitated regional efforts to develop the *Blueprint for entrepreneurial growth and economic prosperity in Southwest Virginia* as well as the *Blueprint for attracting and sustaining advanced manufacturing in Southwest Virginia*. She serves on the Virginia Rural Council Board and is leading SWVA's efforts as part of the White House TechHire designation program. Prior to joining the UVa-Wise team, she served as a Senior Project Manager with the Virginia Department of Business Assistance, where she coordinated local, regional, and state efforts in support of the CGI and Northrop Grumman operations in Southwest Virginia. She is an accomplished instructor, consultant, and former director of customer service/operations with twelve years of experience in private industry.

Dr. Guy Duczynski is a national security professional with 25 years of service with Special Operations, including two operational tours in the counter-terrorism unit of the Australian Special Air Service (SAS). He served in operations, plans, training, and development branches before retiring from military service in 2002. In addition to a doctorate, he holds a master's degree in Business Administration and a master's degree in Education. He continues research in effects-based operations, planning, information operations, capability development, and special operations, and lectures regularly to strategic-level planners. He is also a senior lecturer to doctoral students undertaking research in information warfare.

Dr. Ruben Elamiryan is the Assistant to the Chair of Political Governance and Public Policy at the Public Administration Academy of the Republic of Armenia. He is also a lecturer at Russian-Armenian (Slavonic) university, and holds a doctorate in Political Science. His research interests include information and cyber security, political globalisation, and geopolitics of the South Caucasus and the Greater Eurasia.

Robert Guess is currently an Associate Professor of Information Systems Technology at Tidewater Community College (TCC), where he has led the development of cyber security, virtualisation, and cloud computing curricula and programs. He earned a bachelor's degree from Virginia Commonwealth University in 1992 and a master's degree in Information Assurance (MSIA) from Norwich University in 2006.

Craig Jackson is Chief Policy Analyst at the Indiana University Center for Applied Cybersecurity Research (CACR), where his research interests include information security program development and governance, cyber security assessments, legal and regulatory regimes' impact on information security and cyber resilience, evidence-based security, and innovative defences. He is a Co-PI of the NSF Cybersecurity Center of Excellence, and leads CACR's collaborative efforts with Naval Surface Warfare Center, Crane, where he is presently employed as temporary faculty. He is the co-author of *Security from first principles: A practical guide to the information security practice principles*. He is a graduate of the IU Maurer School of Law, IU School of Education, and Washington University in St. Louis. In addition to his litigation experience, his research, design, project management, and psychology background includes work at the IU Center for Research on Learning and Technology and the School of Medicine at Washington University in St. Louis.

Dr. Charles Knight is a practitioner-academic who teaches in the postgraduate terrorism and security program at Charles Sturt University. He first served as a regular officer in the British Army, later spending four years with the Omani Army and delivering counterinsurgency training in operational settings in Asia—which informed his doctoral research on repression and popular support in asymmetric conflict. In Australia he held senior management positions in the security arena and continues to serve as a reservist—having previously commanded an infantry battalion and held both operational and development staff appointments. In the latter he developed capability and futures analytic methods which led to his research on emotional bias in decision-making. As a long-standing specialist in urban operations, he developed simulation systems, wrote the Army's doctrine, and drove the adoption of new training methods, bringing an applied understanding to his research on the evolving nature of complex conflict.

Dr. Alexander Kott serves as the U.S. Army Research Laboratory's (ARL) Chief Scientist in Adelphi, Maryland. In this role he provides leadership in the development of ARL technical strategy, maintaining technical quality of ARL research, and representing ARL to the external technical community. From 2009-2016 he was the Chief, Network Science Division, Computational and Information Sciences Directorate at ARL, responsible for fundamental research and applied development in network science and science for cyber defence. Prior to that, from 2003-2008, he served as a Defense Advanced Research Programs Agency (DARPA) Program Manager. His earlier positions included serving as Director of R&D at the Carnegie Group, in Pittsburgh, Pennsylvania. There, his work focused on novel information technology approaches to complex problems in engineering design, and planning and control in manufacturing, telecommunications, and aviation industries. He earned a doctorate in Mechanical Engineering from the University of Pittsburgh in 1989, where he researched Artificial Intelligence approaches to invention of complex systems. He received the Secretary of Defense Exceptional Public Service Award in October 2008. He has published more than 80 technical papers and served as the co-author and primary editor of more than ten books. His columns "The Internet of Battle Things" and "The Fog of War in Cyberspace" appeared in IEEE Computer in 2016.

Dr. Mamikon Margaryan is a lecturer at the Chair of Political Governance and Public Policy at the Public Administration Academy of the Republic of Armenia. He is also a political expert with the Republican Party faction at the National Assembly of the RA. He earned a doctorate in Political Science. He is the author of the monograph, *The issues of political stability and national security in Armenia*. His research interests include the modernisation of domestic political processes and national security.

Dr. Alessandro Oltramari is a Research Scientist and Project Lead at the Bosch Research and Technology Center (Pittsburgh, PA, USA), where he works on intelligent systems and semantic technologies. Prior to this position, he was a Research Associate at Carnegie Mellon University (2010-2016). He also held a research position at the Laboratory for Applied Ontology (ISTC-CNR) in Trento (Italy) from 2000 to 2010. He was a Visiting Research Associate at Princeton University in 2005 and 2006. He earned his doctorate in Cognitive Science and Education from the University of Trento, in co-tutorship with the Institute for Cognitive Science and Technology of the Italian National Research Council (ISTC-CNR). His primary research interests are centred around theoretical and applied research on knowledge representation and cognitive technologies.

Dr. Neil C. Rowe is a Professor of Computer Science at the U.S. Naval Postgraduate School (Monterey, CA, USA), where he has been since 1983. He earned a doctorate in Computer Science from Stanford University (1983). His main research interests are data mining, digital forensics, modelling of deception, and cyberwarfare.

Scott Russell is a Senior Policy Analyst at the Indiana University Center for Applied Cybersecurity Research (CACR), where his work focuses on the improvement of federal privacy and cyber-security policy. A lawyer and researcher, he specialises in privacy, cyber security, and international law, and his past research has included principled cyber-security, cyber-security assessments, international cyber-security due diligence, cyber-security self-governance regimes, international data jurisdiction, and digital surveillance. He is a co-author of *Security from first principles: A practical guide to the information security practice principles*, and is a key contributor to CACR's collaborative efforts with Naval Surface Warfare Center, Crane, where he currently serves as temporary faculty. He earned his bachelor's degrees in Computer Science and History from the University of Virginia, and earned his J.D. from Indiana University. He previously interned at MITRE and served as a postdoctoral fellow at CACR.

Agnija Tumkevič is a doctoral student at Vilnius University, where she has studied international security, strategic studies, and diplomacy. Her research focuses on cyber-security issues, and, in particular, the conditions under which countries cooperate with each other in the cyber domain. She also works at the Ministry of Foreign Affairs of the Republic of Lithuania.

Operating in the Dark: Cyber Decision-Making from First Principles

SL Russell, SC Jackson

Center for Applied Cybersecurity Research
Indiana University
Bloomington, Indiana, USA

E-mail: scolruss@indiana.edu; scjackso@indiana.edu

Abstract: *The future of cyber conflict will present an uncertain, insecure, and rapidly changing environment. Cyber security will prove to be increasingly important for the defence community, and cyber literacy will be necessary for an increasing number of decision-makers. To continue to achieve its mission, the defence community should rally around a doctrinal set of first principles. The authors propose the Information Security Practice Principles as a foundational text to serve at the highest tier of analysis for defence cyber decision-making.*

Keywords: *Cyber Security, Cyber Decision-Making, Defence, First Principles, Information Security Practice Principles*

Introduction

The future of cyber conflict goes far beyond the mouse and keyboard, or even ones and zeroes. As a domain, cyber spans the spectrum of conflict, from low-level information warfare to multi-domain hot wars with cyber operating in tandem with air, land, sea, and space. Cyber attacks increasingly have life or death consequences, as mission-critical functions increasingly connect to global networks. Cyber operations frequently exploit new systems critical to national security (Fidler 2017). Cyber literacy, once relegated to technical specialists, is now a capability required across the defence community. Decision-makers up and down the chain of command will need the ability to quickly comprehend, assess, and communicate cyber priorities and cyber-security concerns. Success in this cyber-enabled conflict depends upon the ability to rally around a solid doctrinal foundation for robust cyber decision-making.

To meet the needs of a changing and increasingly complex environment, the defence community should rally around a set of principles for cyber decision-making. The Information Security Practice Principles fill a serious gap in contemporary cyber-security doctrine and should serve as the highest tier of analysis for all defence cyber decision-making (Jackson, Russell & Sons 2017). While not sufficient for comprehensive cyber security, the adoption of the Principles is necessary for the defence community to continue to achieve its mission in an increasingly connected, complex, and vulnerable operational environment.

This article identifies the contemporary trends that will make cyber security an increasingly prominent challenge for the defence community in the near and mid-term future. It then introduces the Information Security Practice Principles, discusses the research and development that went into the Principles, and examines how the Principles can be used by the defence community to offset the trends identified.

Contemporary Trends Will Make Cyber Security and Resiliency More Difficult in the Future

Trends with momentum today will serve as the foundation for the challenges of tomorrow, and managing the following trends will be essential to cyber decision-making: (1) the increasing attack surface and complexity of the battlespace for cyber conflict, (2) the increasing influence of non-defence actors on defence decision-making, (3) the increasing necessity of cyber literacy up and down the chain of command, and (4) the continuing importance of non-cyber interests in cyber decision-making.

It is tempting to hypothesise about technological game changers—artificial intelligence, quantum computing—and how they will revolutionise cyber security. The authors take a more pragmatic approach. As a baseline, they do not assume that contemporary cyber-security challenges will be resolved by a sea change in technology, policy, or international relations. They also do not assume that cyber defence will catch up to cyber-offensive innovation or investment anytime soon. Nor do they assume that the longstanding trend lines underlying cyber security will change course.

The attack surface and complexity of the battlespace is increasing

The contemporary battlespace is undergoing a substantial expansion in both attack surface and complexity, and current trend lines suggest that this is going to get much worse. Nearly every conception of future conflict expects far greater reliance on networked operational systems, and most long-term research and development plans assume some version of a 'connected battlespace', in which networked technology serves as the backbone for advanced warfighting (Lagrone 2016). The logic behind this development is straightforward: greater connectivity of combat systems enables a tremendous increase in combat capabilities, particularly as combat grows increasingly reliant on autonomous, semi-autonomous, and remotely-controlled warfighting technologies. Warfighters of the future will be more reliant on machines than ever before, serving as "quarterbacks setting up the play, while the rest of the team—the machines—carry it out" (Lapowsky 2017).

This surge in capabilities comes with a surge in vulnerabilities, as the connectivity that facilitates this new paradigm necessarily expands the scale, complexity, and attack surface for hostile cyber operations to exploit. Cyber attackers already enjoy an asymmetric advantage built around asynchronicity, near-instant timescales, and a global Internet (Phillips 2012). Expanding attack surface and complexity gives attackers more points of attack and more cover under which to hide. Cyber security fundamentally suffers when the defenders cannot keep up with the size and complexity of the systems they are tasked with defending. And as defenders fall behind, attackers thrive. After all, defenders need to protect the entirety of their systems, whereas attackers may need only one flaw.

Moreover, as weapons increasingly look like computers, they are increasingly vulnerable to cyber-disruption, just as computers are. While cyber attacks have historically been constrained to traditional computer networks, the explosion of Internet-of-Things (IoT)-style networked devices means that cyber vulnerabilities will arise from nearly every part of the connected battlespace, thus creating a veritable hackers' playground. In the past, even if computer networks went down, the warfighters' weapons would still fire. The dramatic expansion in the use of networked technologies in previously analogue systems dramatically increases the potential impact of cyber attacks.

This expansion of the military attack surface in many ways mirrors the advent of the 'total war' in the 20th century. Airplane mobility opened up the economic foundries supporting nation-states' war efforts as legitimate targets, which fundamentally reshaped the conception of the military battlespace. As in the total war, the recent expansion in networked technology has opened new avenues of attack, which has targeted the defence industry's increasing reliance on private-sector infrastructure. As with the total war, cyber conflict will require not only the defence of the connected battlespace, but also the defence of large swathes of the private sector and the non-defence public sector.

Presidential policy directive 63 established the importance of critical infrastructure for US defence and national security, and began the long and difficult task of attempting to secure this infrastructure from cyber attack (White House 1998). Developments such as the Defense Critical Infrastructure Protection Program re-emphasise the importance of private infrastructure on the performance of defence systems (Government Accountability Office 2008), and an ever-increasing number of private-sector entities are proving critical for national security (White House 2013). Protecting this wider array of defence-adjacent industries is already a daunting task, and the scale and complexity of the infrastructure needing protection is only likely to increase in the future.

The increasing importance of private-sector-controlled infrastructure is also a manifestation of the second trend highlighted here: the growing influence of non-defence perspectives on defence cyber decision-making.

The influence of non-defence actors is increasing

Defence decision-makers are increasingly looking to non-defence sectors as a model for cyber decision-making on issues ranging from increasing reliance on commodity Information Technology (IT), to adopting non-defence risk-management and risk-governance frameworks, to shifting business practices toward those utilised by Silicon Valley. This greater reliance on non-defence perspectives in security-critical areas raises a host of challenges, particularly considering the commercial private sector's poor track record on cyber security.

The increasing influence of and reliance on non-defence actors is perhaps best seen in the increasing utilisation of private-sector commodity IT. The quintessential example is the smartphone. Commercial smartphone technology has seen tremendous advances. It makes sense that the defence community would take advantage of this powerful technology. The commercial private sector is renowned for its potential to innovate new capabilities, and often these capabilities overlap with the needs of the defence community. Nevertheless, the increasing outsourcing of IT manufacturing raises substantial cyber-security concerns. For instance, identifying and securing the complete chain of custody for each IT component has made supply-chain security a prodigious cyber-security problem (Baldwin 2014). Considering the loss of the 'trusted foundry', the increasing globalisation of the IT supply chain, and the substantial increase in the use of networked

IT discussed above, the cyber security of nearly every aspect of the connected battlespace should be called into question (McCormack 2016).

This trend goes beyond adopting technology, as the defence community increasingly looks to Silicon Valley for business practices and processes to spur rapid innovation. The Defense Innovation Unit Experimental (DIUx), the US Department of Defense (DoD) Rapid Innovation Fund, the Defense Innovation Board, and the DoD Strategic Capabilities Office all share the mindset that concerted, rapidly-paced development projects will be central to strategic advantage. This mindset can be seen filtering down through the larger defence Research and Development (R&D) apparatus. By modelling the development practices of Silicon Valley, these organisations hope to more rapidly bring novel capabilities to operational usage. Yet as history has taught, this speed often comes at the expense of cyber security. By adopting this approach to system development, these organisations may be baking in architectural vulnerabilities in technologies that will threaten mission success for years to come. Although the business practices of Silicon Valley may offer tremendous benefit to the defence community, these practices will also need to incorporate foundational security considerations.

Finally, the influence of non-defence perspectives is seen with the US Department of Defense's recent move to adopt the cyber-security standards developed by the Department of Commerce's National Institute of Standards and Technology (NIST). Since the passage of the Federal Information Security Management Act (FISMA) in 2002, NIST has generated the cyber-security standards utilised by the federal government—apart from 'national security systems'—collectively referred to as the Risk Management Framework (RMF). In 2014, NIST and private-sector stakeholders also developed and published the private-sector-focused Cybersecurity Framework (CSF). In 2014, the Department of Defense announced its intention to adopt RMF and move away from the previous Defense Information Assurance Certification and Accreditation Program (DIACAP) standards (Department of Defense 2014). And most recently, President Trump signalled that the federal government would begin looking to use CSF as the primary framework governing cyber security, with uncertain ramifications for the defence and intelligence communities (White House 2017).

While there is much to be explored regarding the effectiveness and efficiency of NIST's cyber-security approaches, the single most important point for the defence community is that these frameworks were developed by and for non-defence organisations. NIST's directive in FISMA explicitly excluded national security systems, and the expertise at NIST has never been considered to extend to defence. The frameworks themselves are ill-suited for the needs of combat systems, as both frameworks operate primarily by prescribing generic control sets based on blunt determinations of risk. As applied, auditors rarely embrace a genuine risk-management approach to cyber security and treat the control sets as massive checklists. Indeed, Acting Deputy Assistant Secretary of Defense (DASD) for Systems Engineering (SE) Kristen Baldwin recently laid out the shortcomings of using RMF to operationalise security for weapons systems, a task neither RMF nor CSF was designed to do (Baldwin 2017).

The importance of cyber literacy up and down the chain of command is increasing

Cyber issues have steadily grown in importance in the defence community: cyberspace is the fifth domain of conflict (‘War in the fifth domain’ 2010); cyber capabilities are cited as a potential third offset (Livingston 2016); the US Cyber Command (USCYBERCOM) has been a combatant command since 2009; and cyber policy issues are frequently addressed by the president. This trend is not isolated to the community of cyber specialists. From the on-the-ground warfighter making tactical calls to flag officers determining broader strategy, all decision-makers need to be able to identify, think about, and communicate cyber-security concepts, concerns, and priorities in a way that is simple and widely understood.

Despite this clear need for widespread cyber literacy, few tools exist to aid decision-makers in understanding and translating cyber issues. At its core, cyber security suffers from a basic translational problem, as the widespread need for cyber literacy is met primarily with narrow, technical language about ‘controls’. These controls, although critical to effective cyber security, can be difficult even for technically savvy personnel to fully grasp and apply to tasks such as mission planning, system design, and policy making. Understanding how control sets implicate broader organisational concerns has been an enduring struggle in cyber security.

The current approach to this translational problem relies on frameworks to structure control selection for senior leadership, often without allowing for meaningful consideration of what controls do, why they are important, or what trade-offs they entail. Despite incorporating terms such as ‘risk management’, these frameworks have, in practice, trended toward compliance because decision-makers do not have the tools to contextualise individual controls in the broader organisational mission. While cyber-security frameworks are not without value, they do not help decision-makers think critically about cyber security.

Conversely, the standards and policies set at the senior leadership level can be equally difficult to distil into technical or procedural requirements. High-level policy language, although superficially appealing, is rarely clear as to how it translates into the realities of hardware, code, and human behaviour. The practical effect of this communication breakdown is that the on-the-ground engineers and operators are left to interpret what they believe constitutes ‘adaptive’ or ‘resilient’, whereas management doubles down on the standards that can be enforced: specifically, compliance-oriented control sets.

Finally, the importance of cyber literacy is reflected in the broader push toward developing a culture of cyber security and resilience. A recurring recommendation from the Defense Science Board has been the need to develop cyber proficiency even among non-cyber professionals, with emphases on training, education, and developing a culture of security (Defense Science Board 2013). These recommendations reflect the growing importance of cyber issues for a wide range of decision-makers, as well as the importance of embedding cyber literacy throughout the defence community. Cyber security needs a baseline of cyber literacy that is accessible and meaningful from the technical and tactical level up to senior leadership. While specialised training will always be important for specific issues, framing those specialised trainings in terms that are universally understood will help break down organisational silos and make cyber security a unified organisational effort.

Cyber security will not be the controlling interest

Finally, despite cyber security's growing importance, it will continue to be balanced against other competing interests and higher-order concerns. Cyber security is a means to support and ensure the needs of the mission and will always be just one factor in a multi-factor calculus. Indeed, the trends identified above, although problematic from a cyber-security perspective, may represent reasoned trade-offs between the benefits of increasing capabilities and the drawbacks of increasing vulnerability. However, it is not clear that the current approach to cyber decision-making reflects this reasoned, nuanced perspective. The authors' goal is not to upend existing trends, but to ensure that the cyber-security concerns they present are fully considered. The importance of these balancing decisions necessitates a robust and adaptable methodology for considering cyber security's competing interests, where the trade-offs are clearly identified and explicitly considered.

Cyber Decision-Making from First Principles

To respond to these structural trends, this article proposes a model for cyber decision-making based on first principles: specifically, the Information Security Practice Principles, which are hereafter referred to as simply the 'Principles'. The Principles are a foundational analytical tool for addressing cyber security. They fill a serious gap in cyber doctrine and will prove particularly important for the defence community where the stakes are high, the potential adversaries are many, and complexity and rapid change are the norm. The Principles are evidence-based, universal, scalable, and actionable. They can also form the foundation for all cyber decision-making activities.

This section introduces the Principles, briefly discusses the research methods and their origin, and explains why the Principles will be particularly valuable for decision-making in future conflicts. The section concludes by providing an in-depth discussion of how the Principles can be applied to defence cyber decision-making.

The seven Principles and the questions they address (see Appendix A) are as follows:

1. **Comprehensivity –** Identify and account for all relevant systems, actors, and risks in the environment. "Am I covering all of my bases?"

2. **Opportunity –** Take advantage of the actor relationships, material resources, and strategic opportunities available in the environment. "Am I taking advantage of my environment?"

3. **Rigor –** Specify and enforce the expected states, behaviors, and processes governing the relevant systems and actors. "What is correct behavior, and how am I ensuring it?

4. **Minimization –** Minimize the size, quantity, and complexity of what is to be protected, and limit externally facing points of attack. "Can this be a smaller target?"

5. **Compartmentation –** Isolate system elements, and enable and control the interactions that are strictly necessary for their intended purposes. "Is this made of distinct parts with limited interactions?"

6. **Fault Tolerance –** Anticipate and address the potential compromise and failure of system elements and security controls. "What happens if this fails?"

7. **Proportionality –** Tailor security strategies to the magnitude of the risks, accounting for the practical constraints imposed by the mission and the environment. “Is this worth it?”

Development

The Principles were developed by a multidisciplinary team of technical, policy, legal, and process experts at Indiana University’s Center for Applied Cybersecurity Research (CACR). This team’s purpose was to identify the underlying and invariant principles informing information security—those which have guided information-security decision-makers across technologies, sectors, and epochs. Information security is not a solved problem. It is a dynamic, multi-disciplinary domain, in which defenders are tasked with complex decision-making scenarios. Despite this inherent complexity, the information-security canon focuses on highly-detailed, narrowly-applicable, and highly-prescriptive resources. Resources of this kind can be valuable, particularly when best practices are well-defined, but they do not help anyone learn to think like an information-security practitioner.

At the outset of their research, the authors discovered many traces and partial attempts to articulate cyber first principles. They found many discussions of principles that only pointed to security controls, truisms, or restatements of ‘best of the best’ practices. They could not find an authoritative source on cyber security’s first principles, so they set out to research and develop these principles themselves.

The baseline criteria established to qualify as ‘principles’ were (1) the Principles must be grounded in prior work; (2) the Principles must guide decision-making; (3) the Principles must predict and describe security outcomes; (4) the Principles must be internally consistent; and (5) the Principles must be generally applicable across time and space. Based on these criteria, the authors conducted an exhaustive literature review of information security and related fields, and iteratively refined their work until settling on the current selection of principles.

As such, the Principles do not purport to be a ‘new’ development in information security, strictly speaking. Rather, they are a collection and meta-analysis of the scope and history of information-security resources, distilled into a discrete, comprehensive, concrete, and practical set of imperatives. The Principles can be found in the wisdom of ancients, dating back to Sun Tzu, as well as in the newest information-security best practices. While the existence of these Principles is not new, their articulation is.

Attributes

The criteria the authors set for the Principles gives them a number of attributes that will likely become increasingly important for future conflict. First and foremost, the Principles are universal and timeless and, therefore, generally applicable across time, space, and domain. Put simply, the Principles do not go out of date or become obsolete. Specific technologies, best practices, and frameworks may come and go, but the Principles offer a methodology that will always be meaningful and will always serve as a jumping-off point for more narrow cyber-security practices in the future.

Second, the Principles guide decision-making. A recurrent shortcoming of other sources identified in this research was that they were not actionable. These other principles would state broad, policyoriented goals, but would not specify how the practitioners must or should carry them out. For instance, the Organization for Economic Co-operation and Development (OECD) established 'Democracy' as a principle, stating that "[t]he security of information systems and networks should be compatible with essential values of a democratic society" (Organization for Economic Co-operation and Development 2002). Although a noble goal, such a principle is difficult to implement at a practical level.

By contrast, the Information Security Practice Principles are designed specifically to guide decision-making. Each principle is structured as an imperative, which instructs practitioners how to implement it, and each principle is paired with a 'self-question', which provides a simple rhetorical device for practitioners to ask themselves to help determine if they are correctly considering the scope and breadth of the principle. Perhaps more importantly, the Principles can be used in real time, which allows for detection of, responses to, and recovery from emerging incidents before they escalate. While more sophisticated decision-making processes will require more specialised training to tackle all of the nuances presented, the baseline Principles-assessment provides a robust and meaningful methodology for assessing cyber-security concerns.

Third, the Principles create an intellectual foundation for confronting the unknown. They offer a grounded foundation for confronting future uncertainty through adherence to timeless principles. They also present a mental model, and their use is fundamentally about structuring human decision-making to benefit security.

Finally, the Principles can be utilised in combination with other competing interests. Although discrete, they are not to be taken in isolation. Each of the Principles has numerous interactions with the others; and by considering the Principles in concert, decision-makers are able to quickly and effectively consider high-level trade-offs and priorities. For instance, when 'resilience' is of particular importance, the principles of Compartmentation, Fault Tolerance, and Rigor must be given particularly strong weight. The reasoning here is straightforward: resilience assumes a world in which adversarial accesses and exploits are unavoidable and prioritises continued operability in the face of attack. Compartmentation enables this by creating systems that prevent the compromise of one element from spreading further than necessary; Fault Tolerance does so by anticipating failures and enacting appropriate safeguards; and Rigor does so by building processes that quickly and effectively respond to attacks and remediate those vulnerabilities. While each principle provides meaningful analysis, understanding these high-level interactions allows decision-makers to discuss cyber priorities and trade-offs in a way that is easily grasped, but highly probative for those who have to implement their policies.

The Defence Community Should Adopt the Information Security Practice Principles as the Highest Tier of Analysis for Cyber Decision-Making

An army of principles can penetrate where an army of soldiers cannot.
–Thomas Paine

This article's core recommendation is that the defence community should incorporate the Principles into the highest tier of cyber decision-making. The Principles fill a void in the field of cyber security by offering foundational first principles and represent a powerful addition to the defence community's cyber decision-making needs. The authors believe the Principles should be adopted for five chief reasons: (1) the Principles provide a common language for cyber security; (2) the Principles provide a tool to adapt to a connected battlespace; (3) the Principles will help manage the growing influence of non-defence actors; (4) the Principles are readily adopted; and (5) the Principles make room for non-cyber priorities. As the future becomes increasingly susceptible to technological disruption, decision-makers need a source to look to that is valuable in any scenario, for any technology, and in the face of profound uncertainty. The Principles fill this niche perfectly and offer the defence community a foundational baseline for all of their cyber decision-making needs.

The authors expect the Principles to be supplemented by a wide range of more specialised and detailed training, policies, and implementation tools, some of which are in development. By utilising the Principles as the foundational analysis, decision-makers will be able to ensure that these more specialised documents fit together to build a broader, more cohesive cyber-defence strategy.

The Principles will provide a basic common language for cyber security

The Principles offer a common language with which all decision-makers can discuss cyber security. Specific cyber-security challenges share commonalities that are universal to the discipline. For instance, most major data breaches represent a failure of Compartmentation, in which a single vulnerability proved sufficient to grant an attacker extensive access to the underlying system. The Principles state these commonalities explicitly, such that specific security concerns can be understood in terms that are universally meaningful. This universality makes the Principles ideally suited for translating between the wide variety of actors with cyber-security concerns. Senior leadership and technical specialists do not need to understand the intricate details of each others' work. They only need to understand each others' high-level concerns and how they intersect. By abstracting away the details and fixating on the fundamentals, the Principles provide a simple mechanism for translating cyber security across all of the defence community and enabling commanders' intents (Storlie 2010; Shattuck 2002).

The Principles' value as a common language is key to addressing the expanding role that cyber security will play in a wide range of non-technical positions. Cyber security has never been exclusively a technical endeavour, but the future will bring about a significant expansion of cyber-security concerns for non-cyber roles (for example, commanders in joint operations in which cyber is one domain). The Principles address this growing need by providing a simple and straightforward lexicon for non-cyber decision-makers to contextualise and communicate cyber issues. Soldiers will need to communicate quickly and effectively about threats and opportunities they are faced with; system designers and acquisitions personnel will need to be able to highlight and discuss high-level design considerations; and senior leadership will need a lexicon for discussing cyber issues that maps high-level concerns across the varied disciplines they oversee. The Principles provide a unified mechanism for ensuring that everyone is on the same page by providing a single common language that is universally meaningful and that immediately conveys high-level cyber-security concerns.

Beyond providing this common language, the Principles also provide an introductory text for expanding cyber literacy. As discussed previously, future conflict will see a dramatic increase in the need for cyber literacy from non-cyber specialists, and the Principles are well-suited to support training in this area. Practitioners versed in the Principles will understand the basic cyber-security considerations that come into play in every scenario and will know what questions to ask when confronted with new cyber-security challenges. Although each discipline will require more specialised training, the Principles provide a solid foundation of cyber literacy by creating a baseline applicable to all of cyber security.

Even among the technically trained, cyber security can be a muddy and poorly articulated discipline, with experts being largely self-taught, closely mentored, or innately gifted. While these methods of learning should not be discounted, they also do not and have not scaled with the need for cyber-security practitioners. The Principles can, therefore, also serve a pivotal role in the broader push for cyber-security training and readiness by providing a robust core of knowledge as the foundation for broader cyber-security education efforts.

The Principles will provide a tool to adapt to the connected battlespace

The Principles offer a powerful tool for cyber decision-makers to confront the uncertainty and insecurity of a highly-connected battlespace. Relying on established practices (or waiting for evidence-based practices to solidify) will not be a viable option for scenarios in which the status quo frequently gives way to disruption. In these scenarios, the best practice for confronting the unknown will be reliance on principled decision-making. The Principles provide a backstop against the future's uncertainty by embedding a baseline, universal model for approaching any scenario.

In addition to providing a universal mental model, Principles-based analysis allows for the rapid consideration of security concerns in time-sensitive operational environments. Practitioners trained in the Principles can apply them in real time, by making tough, timely calls when decisiveness is critical.

More fundamentally, however, the Principles provide an easily accessible mental model for approaching the complexities of the connected battlespace. Even for well-known cyber-security problems, an established path forward is not always clear. Decision-makers need a sound basis for making judgment calls in these complicated scenarios. When faced with sufficiently complex systems, outcomes will never be entirely clear or predictable, and tools will be needed to aid decision-makers in confronting these complexities (Bar-Yam 2002). For a non-cyber example, physicians are frequently confronted with complex scenarios for which best practices are not clearly established; hence, the physicians are forced to make judgment calls. This skillset—combining training, experience, and fundamentals to approach complex situations—is a hallmark of the traditional 'professions' and is something that cyber security will need to confront the complexities of in the connected battlespace. While the Principles alone are not enough, they are an invaluable step in creating a class of cyber practitioners who can confront the complexities the future of cyber conflict will present.

The Principles will help manage the growing influence of non-defence actors

The Principles will provide a foundation for managing the growing influence of non-defence actors in defence decision-making by providing a language for communicating priorities, a tool for identifying and analysing vulnerabilities, and a model for adapting to operational insecurities.

Defence acquisitions is one key area the Principles can aid in this regard. The Principles provide numerous functions of critical importance to the acquisitions process, including identifying and communicating cyber-security priorities and standards, providing a consistent analysis for cyber security throughout system lifecycles, structuring the assessment of cyber-security systems and programs, and serving as a foundation for training and readiness for acquisitions personnel. The Principles' adaptability and universality make them an ideal baseline for all cyber assessments in acquisitions, and the Principles' accessibility and usability make them ideal for deployment among the vast array of cyber and non-cyber personnel needed.

Moreover, the Principles provide a broader, more holistic methodology for the management of cyber-security frameworks. As previously discussed, non-defence cyber-security frameworks are playing an increasingly important role in defence decision-making, despite being designed for non-defence environments. The Principles can help alleviate this misalignment by providing a high-level overlay onto these frameworks, one that allows defence decision-makers to think critically about how the application of non-defence frameworks should be contextualised for defence purposes. Although the framework may lay out a baseline set of controls, the Principles can be used to communicate higher-order priorities; to identify shortcomings and incongruities; and, therefore, to govern how those frameworks are ultimately implemented.

By understanding the high-level security concerns that decisions implicate, decision-makers will be empowered to think critically about the ramifications of their actions, and to take steps to address those ramifications. The Principles do not require the wholesale removal of non-defence perspectives from defence decision-making. Quite to the contrary, the principle Proportionality specifically makes room for the consideration of competing interests that cyber security implicates. Adopting the Principles will enhance defence decision-makers' analysis of the trade-offs presented by the growing influence of non-defence perspectives and will provide tools to push back when necessary. Furthermore, the Principles provide a high-level framework for combatting the negatives presented. For instance, the Principles teach that when the scale and complexity of systems cannot be restrained (a failure of Minimization), practitioners should place greater reliance on Compartmentation, Comprehensivity, and Fault Tolerance.

The Principles are readily adopted

The Principles will prove valuable to the defence community because they provide a powerful cyber-security resource with minimal cost or disruption. They supplement, not supplant, existing cyber-security decision-making processes by filling a void in information security: the lack of foundational first principles. Adoption of the Principles neither requires abandoning existing cyber-security frameworks or policies, nor necessitates changing course on the trends identified above. No matter what decision-makers are currently doing, they can use the Principles, too, and will benefit from doing so. The Principles provide a lens for analysing current and future practices, at the same time that they provide a methodology for determining which practices are beneficial and which should be eliminated.

Moreover, because of the Principles' foundational nature, they are easily incorporated across the spectrum of cyber-security training. The Principles are accessible regardless of technical expertise and are designed to be usable by anyone with a need or interest in cyber security. This accessibility means that the Principles are not just easily overlaid onto governing frameworks and policies, but they are also easily incorporated throughout the communities in which they are adopted. Technical cyber-security specialists will not be lost in vague policy language that is difficult to parse and impractical to implement; nor will managers and policymakers be subjected to technical jargon and control-heavy standards that are difficult to understand in the context of their organisational function.

The Principles make room for non-cyber issues

Finally, despite the growing importance of cyber-security issues to defence decision-making, cyber security is not the only issue and cyber is certainly not the only warfighting domain. Cyber should not take up a disproportionate amount of decision-makers' time and resources. The Principles allow for cyber decision-makers to understand, think about, and convey cyber-security priorities without getting bogged down in excessive detail or falling back to immature checklist-oriented approaches that assume all decisions can be made *a priori*. Put simply, the Principles will do what needs to be done, and then they will get out of the way.

Conclusion

The Information Security Practice Principles represent a powerful addition to the defence community's cyber-security and resiliency capability. Their foundational nature and universal applicability make them, among other things, an ideal basis for cyber-training and readiness, a common language for cyber-security communication, an analytical framework for cyber decision-making, and a core document for specification and assessment in cyber acquisitions. The challenges posed by future cyber conflict will require adaptive, principled human decision-making schooled in foundations of information security, and the Information Security Practice Principles offer an indispensable resource toward achieving that goal.

Acknowledgements

The authors would like to thank Robert Templeman, Anurag Shankar, Zalak Shah, Ian Washburn, Randy Heiland, Scott Orr, Mike Simpson, Marendar Edunuri, Ryan Kiser, and Matt Estell for their comments. The authors also thank CACR for supporting this work; special thanks go to Susan Sons for her work in the development of the Principles.

References

Baldwin, K 2014, *DoD JFAC overview*, US Office of the Secretary of Defense for Acquisition, Technology and Logistics, 29 October, viewed 3 October 2017, <http://www.acq.osd.mil/se/briefs/16950-2014_10_29_NDIA-SEC-Baldwin-JFAC-vF.pdf>.

——2017, 'Keynote address of Ms. Kristen Baldwin: Engineering cyber resilient weapons systems', *7th Annual Secure and Resilient Cyber Architectures Invitational & Training Event*, MITRE, 9 May.

Bar-Yam, Y 2002, 'General features of complex systems', *Encyclopedia of life support systems*, viewed 3 October 2017, <http://www.eolss.net/sample-chapters/c15/E1-29-01-00.pdf>.

Defense Science Board 2013, *Task force report on resilient military systems and the advanced cyber threat*, viewed 3 October 2017, <http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf>.

Department of Defense 2014, *DoD instruction 8510.01: Risk Management Framework (RMF) for DoD Information Technology*, 12 March, viewed 3 October 2017 <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf>.

Fidler, D 2017, *Transforming election cybersecurity*, Council on Foreign Relations, 17 May, viewed 3 October 2017, <https://www.cfr.org/report/transforming-election-cybersecurity>.

Government Accountability Office 2008, *Defense critical infrastructure: DoD's risk analysis of its critical infrastructure omits highly sensitive assets*, 2 April, viewed 3 October 2017, <http://www.gao.gov/assets/100/95438.pdf>.

Jackson, C, Russell, S, and Sons, S 2017, *The Information Security Practice Principles foundational whitepaper*, Indiana University Center for Applied Cybersecurity Research, viewed 3 October 2017, <https://cacr.iu.edu/principles/>.

Lagrone, S 2016, 'Navy eyeing the 2045 battle space in new long-term R&D plan', *USNI News*, 26 October, viewed 3 October 2017, <https://news.usni.org/2016/10/26/navy-eyeing-2045-battle-space-new-long-term-rd-plan>.

Lapowsky, I 2017, 'The autonomous future of warfare looks a lot like Pokemon Go', *Wired*, 13 March, viewed 3 October 2017, <https://www.wired.com/2017/03/autonomous-future-warfare-looks-lot-like-pokemon-go/>.

Livingston, I 2016, *Technology and the 'third offset' foster innovation for the force of the future*, Brookings Institute, 9 December, viewed 3 October 2017, <https://www.brookings.edu/blog/order-from-chaos/2016/12/09/technology-and-the-third-offset-foster-innovation-for-the-force-of-the-future/>.

McCormack, R 2016, 'DOD, NSA enter a new world order: U.S. is now dependent on foreign companies for its most sensitive electronics', *Manufacturing and Technology News*, 31 May, viewed 3 October 2017, <http://www.manufacturingnews.com/news/2016/Trusted-Foundry-0531161.html>.

Organization for Economic Co-operation and Development 2002, *OECD guidelines for the security of information systems and networks*, 25 July, viewed 3 October 2017, <http://www.oecd.org/sti/ieconomy/15582260.pdf>.

Phillips, A 2012, 'The asymmetric nature of cyber warfare', *USNI News*, 14 October, viewed 3 October 2017, <https://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare>.

Shattuck, L 2002, 'Communicating intent and imparting presence,' *Military Review*, March-April, viewed 3 October 2017, <http://www.au.af.mil/au/awc/awcgate/milreview/shattuck.pdf>.

Storlie, C 2010, 'Manage uncertainty with commander's intent', *Harvard Business Review*, 3 November, viewed 3 October 2017, <https://hbr.org/2010/11/dont-play-golf-in-a-football-g>.

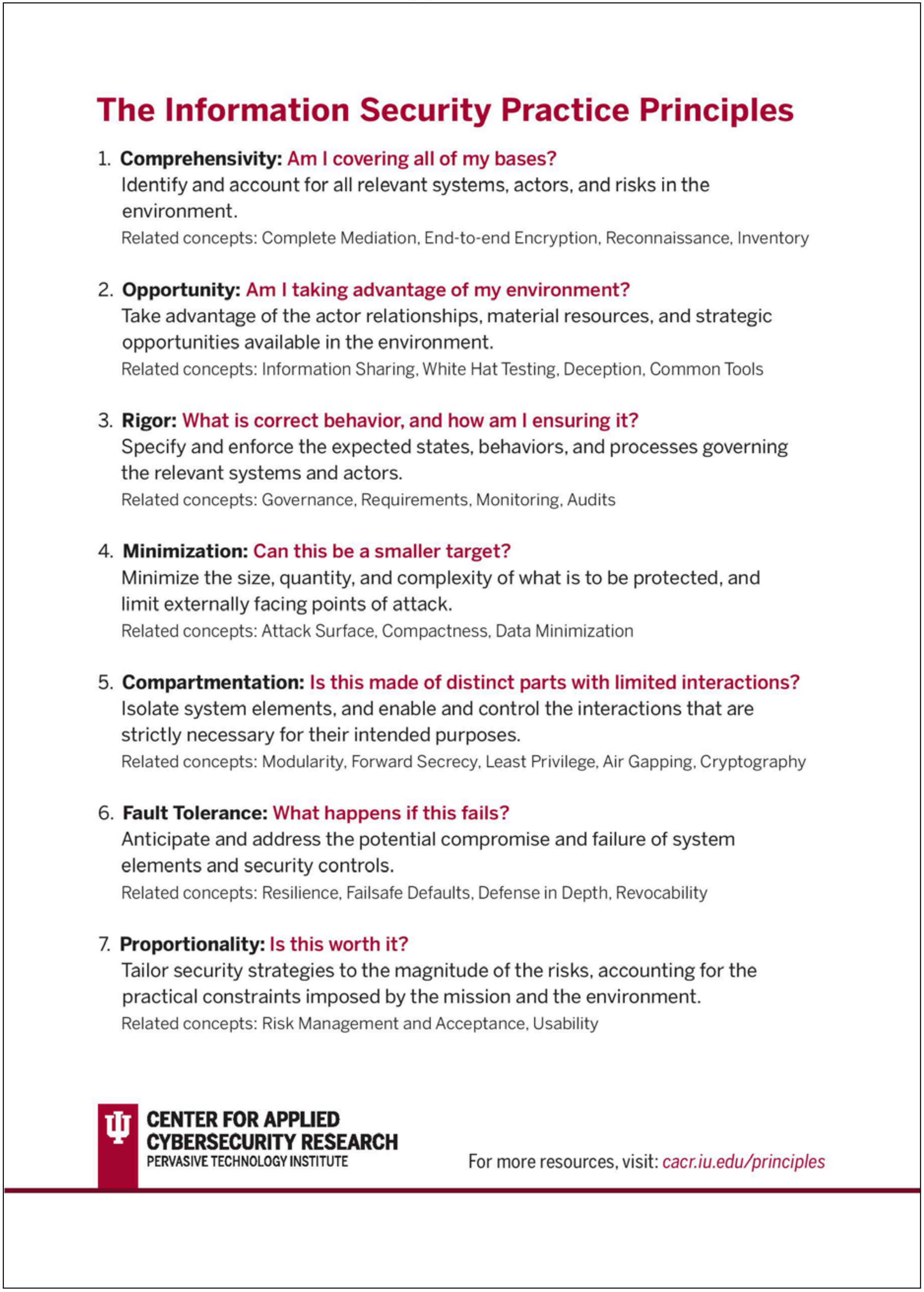
‘War in the fifth domain’ 2010, *The Economist*, 1 July, viewed 3 October 2017, <http://www.economist.com/node/16478792>.

White House 1998, *Presidential policy directive 63: Critical infrastructure protection*, May 22, viewed 3 October 2017, <https://fas.org/irp/offdocs/pdd/pdd-63.htm>.

——2013, *Executive order 13636: Improving critical infrastructure cybersecurity*, 12 February, viewed 3 October 2017, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

——2017, *Presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure*, 11 May, viewed 3 October 2017, <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.

Appendix A



The Information Security Practice Principles

1. **Comprehensivity:** **Am I covering all of my bases?**
   Identify and account for all relevant systems, actors, and risks in the environment.
   Related concepts: Complete Mediation, End-to-end Encryption, Reconnaissance, Inventory

2. **Opportunity:** **Am I taking advantage of my environment?**
   Take advantage of the actor relationships, material resources, and strategic opportunities available in the environment.
   Related concepts: Information Sharing, White Hat Testing, Deception, Common Tools

3. **Rigor:** **What is correct behavior, and how am I ensuring it?**
   Specify and enforce the expected states, behaviors, and processes governing the relevant systems and actors.
   Related concepts: Governance, Requirements, Monitoring, Audits

4. **Minimization:** **Can this be a smaller target?**
   Minimize the size, quantity, and complexity of what is to be protected, and limit externally facing points of attack.
   Related concepts: Attack Surface, Compactness, Data Minimization

5. **Compartmentation:** **Is this made of distinct parts with limited interactions?**
   Isolate system elements, and enable and control the interactions that are strictly necessary for their intended purposes.
   Related concepts: Modularity, Forward Secrecy, Least Privilege, Air Gapping, Cryptography

6. **Fault Tolerance:** **What happens if this fails?**
   Anticipate and address the potential compromise and failure of system elements and security controls.
   Related concepts: Resilience, Failsafe Defaults, Defense in Depth, Revocability

7. **Proportionality:** **Is this worth it?**
   Tailor security strategies to the magnitude of the risks, accounting for the practical constraints imposed by the mission and the environment.
   Related concepts: Risk Management and Acceptance, Usability

CENTER FOR APPLIED
CYBERSECURITY RESEARCH
PERVASIVE TECHNOLOGY INSTITUTE

For more resources, visit: *cacr.iu.edu/principles*