

**Cybersecurity design reduces the risk of system failure from cyberattack, aiming to maximize mission effectiveness.**

BY O. SAMI SAYDJARI

# Engineering Trustworthy Systems: A Principled Approach to Cybersecurity

CYBERATTACKS ARE INCREASING in frequency, severity, and sophistication. Target systems are becoming increasingly complex with a multitude of subtle dependencies. Designs and implementations continue to exhibit flaws that could be avoided with well-known computer-science and engineering

techniques. Cybersecurity technology is advancing, but too slowly to keep pace with the threat. In short, cybersecurity is losing the escalation battle with cyberattack. The results include mounting damages

in the hundreds of billions of dollars,<sup>4</sup> erosion of trust in conducting business and collaboration in cyberspace, and risk of a series of catastrophic events that could cause crippling damage to companies and even entire countries. Cyberspace is unsafe and is becoming less safe every day.

The cybersecurity discipline has created useful technology against aspects of the expansive space of possible cyberattacks. Through many real-life engagements between cyberattackers and defenders, both sides have learned a great deal about how to

## » key insights

- **Cybersecurity must be practiced as a principled engineering discipline.**
- **Many principles derive from insight into the nature of how cyberattacks succeed.**
- **Defense in depth and breath is required to cover the spectrum of cyberattack classes.**

design attacks and defenses. It is now time to begin abstracting and codifying this knowledge into principles of cybersecurity engineering. Such principles offer an opportunity to multiply the effectiveness of existing technology and mature the discipline so that new knowledge has a solid foundation on which to build.


*Engineering Trustworthy Systems*<sup>8</sup> contains 223 principles organized into 25 chapters. This article will address 10 of the most fundamental principles that span several important categories and will offer rationale and some guidance on application of those principles to design. Under each primary principle, related principles are also included as part of the discussion.

For those so inclined to read more in *Engineering Trustworthy Systems*, after each stated principle is a reference of the form “{x.y}” where x is the chapter number in which it appears and y is the y-th principle listed in that chapter (which are not explicitly numbered in the book).


**Motivation**

Society has reached a point where it is inexorably dependent on trustworthy systems. Just-in-time manufacturing, while achieving great efficiencies, creates great fragility to cyberattack, amplifying risk by allowing effects to propagate to multiple systems {01.06}. This means that the potential harm from a cyberattack is increasing and now poses existential threat to institutions. Cybersecurity is no longer the exclusive realm of the geeks and nerds, but now must be considered as an essential risk to manage alongside other major risks to the existence of those institutions.

The need for trustworthy systems extends well beyond pure technology. Virtually everything is a system from some perspective. In particular, essential societal functions such as the military, law enforcement, courts, societal safety nets, and the election process are all systems. People and their beliefs are systems and form a component of larger societal systems, such as voting. In 2016, the world saw cyberattacks transcend technology targets to that of wetware—human beliefs and propensity to action. The notion of hacking democracy itself came into light,<sup>10</sup> posing an existential threat to entire gov-



## Students of cybersecurity must be students of cyberattacks and adversarial behavior.



ernments and ways of life though what is sometimes known by the military as *influence operations*{24.09}.<sup>6</sup>

Before launching into the principles, one more important point needs to be made: *Engineers are responsible for the safety and security of the systems they build* {19.13}. In a conversation with my mentor’s mentor, I once made the mistake of using the word *customer* to refer to those using the cybersecurity systems we were designing. I will always remember him sharply cutting me off and telling me that they were “clients, not customers.” He said, “Used-car salesmen have customers; we have clients.” Like doctors and lawyers, engineers have a solemn and high moral responsibility to do the right thing and keep those who use our systems safe from harm to the maximum extent possible, while informing them of the risks they take when using our systems.

In *The Thin Book of Naming Elephants*,<sup>5</sup> the authors describe how the National Aeronautics and Space Administration (NASA) shuttle-engineering culture slowly and unintentionally transmogrified from that adhering to a policy of “safety first” to “better, faster, cheaper.” This change discouraged engineers from telling truth to power, including estimating the *actual* probability of shuttle-launch failure. Management needed the probability of launch failure to be less than 1 in 100,000 to allow launch. Any other answer was an annoyance and interfered with on-time and on-schedule launches. In an independent assessment, Richard Feynman found that when engineers were allowed to speak freely, they calculated the actual failure probability to be 1 in 100.<sup>5</sup> The engineering cultural failure killed many great and brave souls in two separate shuttle accidents.

I wrote *Engineering Trustworthy Systems* and this article to help enable and encourage engineers to take full charge of explicitly and intentionally managing system risk, from the ground up, in partnership with management and other key stakeholders.

**Principles**

It was no easy task to choose only 5% of the principles to discuss. When in doubt, I chose principles that may be less obvious to the reader, to pique cu-

riosity and to attract more computer scientists and engineers to this important problem area. The ordering here is completely different than in the book so as to provide a logical flow of the presented subset.

Each primary principle includes a description of what the principle entails, a rationale for the creation of the principle, and a brief discussion of the implications on the cybersecurity discipline and its practice.

► **Cybersecurity's goal is to optimize mission effectiveness {03.01}.**

*Description.* Systems have a primary purpose or mission—to sell widgets, manage money, control chemical plants, manufacture parts, connect people, defend countries, fly airplanes, and so on. Systems generate mission value at a rate that is affected by the probability of failure from a multitude of causes, including cyberattack. The purpose of cybersecurity design is to reduce the probability of failure from cyberattack so as maximize mission effectiveness.

*Rationale.* Some cybersecurity engineers mistakenly believe that their goal is to maximize cybersecurity under a given budget constraint. This excessively narrow view misapprehends the nature of the engineering trade-offs with other aspects of system design and causes significant frustration among the cybersecurity designers, stakeholders in the mission system, and senior management (who must often adjudicate disputes between these teams). In reality, all teams are trying to optimize mission effectiveness. This realization places them in a collegial rather than an adversarial relationship.

*Implications.* Cybersecurity is always in a trade-off with mission functionality, performance, cost, ease-of-use and many other important factors. These trade-offs must be intentionally and explicitly managed. It is only in consideration of the bigger picture of optimizing mission that these trade-offs can be made in a reasoned manner.

► **Cybersecurity is about understanding and mitigating risk {02.01}.**

*Description.* Risk is the primary metric of cybersecurity. Therefore, understanding the nature and source of risk is key to applying and advancing the discipline. Risk measurement is foundational to improving cybersecurity {17.04}. Conceptually, cybersecurity risk is

simply the probability of cyberattacks occurring multiplied by the potential damages that would result if they actually occurred. Estimating both of these quantities is challenging, but possible.

*Rationale.* Engineering disciplines require metrics to: “characterize the nature of what is and why it is that way, evaluate the quality of a system, predict system performance under a variety of environments and situations, and compare and improve systems continuously.”<sup>7</sup> Without a metric, it is not possible to decide whether one system is better than another. Many fellow cybersecurity engineers complain that risk is difficult to measure and especially difficult to quantify, but proceeding without a metric is impossible. Thus, doing the hard work required to measure risk, with a reasonable uncertainty interval, is an essential part of the cybersecurity discipline. Sometimes, it seems that the cybersecurity community spends more energy complaining how difficult metrics are to create and measure accurately, than getting on with creating and measuring them.

*Implications.* With risk as the primary metric, risk-reduction becomes the primary value and benefit from any cybersecurity measure—technological or otherwise. Total cost of cybersecurity, on the other hand, is calculated in terms of the direct cost of procuring, deploying, and maintaining the cybersecurity mechanism as well as the indirect costs of mission impacts such as performance degradation, delay to market, capacity reductions, and usability. With risk-reduction as a benefit metric and an understanding of total costs, one can then reasonably compare alternate cybersecurity approaches in terms of risk-reduction return on investment. For example, it is often the case that there are no-brainer actions such as properly configuring existing security mechanisms (for example, firewalls and intrusion detection systems) that cost very little but significantly reduce the probability of successful cyberattack. Picking such low-hanging fruit should be the first step that any organization takes to improving their operational cybersecurity posture.

► **Theories of security come from theories of insecurity {02.03}.**

*Description.* One of the most impor-

tant yet subtle aspects of an engineering discipline is understanding how to think about it—the underlying attitude that feeds insight. In the same way that failure motivates and informs dependability principles, cyberattack motivates and informs cybersecurity principles. Ideas on how to effectively defend a system, both during design and operation, must come from an understanding of how cyberattacks succeed.

*Rationale.* How does one prevent attacks if one does not know the mechanism by which attacks succeed? How does one detect attacks without knowing how attacks manifest? It is not possible. Thus, students of cybersecurity must be students of cyberattacks and adversarial behavior.

*Implications.* Cybersecurity engineers and practitioners should take courses and read books on ethical hacking. They should study cyberattack and particularly the post-attack analysis performed by experts and published or spoken about at conferences such as Black Hat and DEF CON. They should perform attacks within lab environments designed specifically to allow for safe experimentation. Lastly, when successful attacks do occur, cybersecurity analysts must closely study them for root causes and the implications to improved component design, improved operations, improved architecture, and improved policy. “Understanding failure is the key to success” {07.04}. For example, the five-whys analysis technique used by the National Transportation Safety Board (NTSB) to investigate aviation accidents<sup>9</sup> is useful to replicate and adapt to mining all the useful hard-earned defense information from the pain of a successful cyberattack.

► **Espionage, sabotage, and influence are goals underlying cyberattack {06.02}.**

*Description.* Understanding adversaries requires understanding their motivations and strategic goals. Adversaries have three basic categories of goals: espionage—stealing secrets to gain an unearned value or to destroy value by revealing stolen secrets; sabotage—hampering operations to slow progress, provide competitive advantage, or to destroy for ideological purposes; and, influence—affecting decisions and outcomes to favor an adversary's interests and goals, usually at

the expense of those of the defender.


*Rationale.* Understanding the strategic goals of adversaries illuminates their value system. A value system suggests in which attack goals a potential adversary might invest most heavily in, and perhaps give insight into how they will pursue those goals. Different adversaries will place different weights on different goals within each of the three categories. Each will also be willing to spend different amounts to achieve their goals. Clearly, a nation-state intelligence organization, a transnational terrorist group, organized crime, a hacktivist and a misguided teenager trying to learn more about cyberattacks all have very different profiles with respect to these goals and their investment levels. These differences affect their respective behaviors with respect to different cybersecurity architectures.

*Implications.* In addition to informing the cybersecurity designer and operator (one who monitors status and controls the cybersecurity subsystem in real time), understanding attacker goals allows cybersecurity analysts to construct goal-oriented attack trees that are extraordinarily useful in guiding design and operation because they give insight into attack probability and attack sequencing. Attack sequencing, in turn, gives insight into getting ahead of attackers at interdiction points within the attack step sequencing {23.18}.


► **Assume your adversary knows your system well and is inside it {06.05}.**

*Description.* Secrecy is fleeting and thus should never be depended upon more than is absolutely necessary {03.05}. This is true of data but applies even more strongly with respect to the system itself {05.11}. It is unwise to make rash and unfounded assumptions that cannot be proven with regard to what a potential adversary may or may not know. It is much safer to assume they know at least as much as the designer does about the system. Beyond adversary knowledge of the system, a good designer makes the stronger assumption that an adversary has managed to co-opt at least part of the system sometime during its life cycle. It must be assumed that an adversary changed a component to have some degree of control over its function so as to operate as the adversary's inside agent.

*Rationale.* First, there are many op-



**It is much better to assume adversaries know at least as much as the designer does about the system.**



portunities for a system design and implementation to be exposed and subverted along its entire life cycle. Early development work is rarely protected very carefully. System components are often reused from previous projects or open source. Malicious changes can easily escape notice during system integration and testing because of the complexity of the software and hardware in modern systems. The maintenance and update phases are also vulnerable to both espionage and sabotage. The adversary also has an opportunity to stealthily study a system during operation by infiltrating and observing the system, learning how the system works in reality, not just how it was intended by the designer (which can be significantly different, especially after an appreciable time in operation). Second, the potential failure from making too weak of an assumption could be catastrophic to the system's mission, whereas making strong assumptions merely could make the system more expensive. Clearly, both probability (driven by opportunity) and prudence suggest making the more conservative assumptions.

*Implications.* The implications of assuming the adversary knows the system at least as well as the designers and operators are significant. This principle means that cybersecurity designers must spend a substantial amount of resources: Minimizing the probability of flaws in design and implementation through the design process itself, and performing extensive testing, including penetration and red-team testing focused specifically on looking at the system from an adversary perspective. The principle also implies a cybersecurity engineer must understand the residual risks in terms of any known weaknesses. The design must compensate for those weaknesses through architecture (for example, specifically focusing the intrusion detection system to monitor possible exploitation of those weaknesses), as opposed to hoping the adversary does not find them because they are "buried too deep" or, worse yet, because the defender believes that the attacker is "not that sophisticated." Underestimating the attacker is hubris. As the saying goes: pride comes before the fall {06.04}.

Assuming the attacker is (partially) inside the system requires the designer

to create virtual bulkheads in the system and to detect and thwart attacks propagating from one part of the system (where the attacker may have a toehold) to the next. This is a wise approach because many sophisticated attacks, such as worms, often propagate within the system once they find their way in (for example, through a phishing attack on an unsuspecting user who clicked on an attacker's malicious link in an email message).

► **Without integrity, no other cybersecurity properties matter {03.06}.**

*Description.* Cybersecurity is sometimes characterized as having three pillars, using the mnemonic C-I-A: preserving *confidentiality* of data, ensuring the *integrity* of both the data and the system, and ensuring the *availability* of the system to provide the services for which it was designed. Sometimes, cybersecurity engineers become hyperfocused on one pillar to the exclusion of adequate attention to the others. This is particularly true of cybersecurity engineers who have their roots in U.S. Department of Defense (DoD) cybersecurity because confidentiality of classified data is a high-priority concern in the DoD. The reality is that all other system properties depend on system integrity, which therefore has primacy.

*Rationale.* System integrity is the single most important property because, without it, no other system properties are possible. No matter what properties a system may possess when deployed, they can be immediately subverted by the attacker altering the system to undo those properties and replace them with properties desirable to the attacker. This gives rise to the fundamental concept of the reference monitor {20.02}, which requires the security-critical subsystem be correct (perform the required security functions), non-bypassable (so that the attacker cannot circumvent the correct controls to access protected resources), and tamperproof (so the system cannot be altered without authorization).

*Implications.* This primacy-of-integrity principle means that cybersecurity engineers must focus attention on access control to the system as a first priority, including heavy monitoring of the system for any unauthorized changes. This priority extends to the earlier stages of system life cycle such as up-

## The effectiveness of depth could be measured by how miserable it makes an attacker's life.

date distribution and maintenance.

► **An attacker's priority target is the cybersecurity system {19.17}.**

*Description.* Closely following from the primacy-of-integrity principle {03.06} is the criticality of the cybersecurity subsystem. To attack the mission, it is necessary first to disable any security controls that effectively defend against the adversary's attack path—including the security controls that defend the security subsystem itself. Great care must be taken to protect and monitor the cybersecurity subsystem carefully {23.12}.

*Rationale.* The security subsystem protects the mission system. Therefore, attempted attacks on the cybersecurity subsystem are harbingers of attacks on the mission system itself {22.08}. The cybersecurity system is therefore a prime target of the adversary because it is the key to attacking the mission system. Protection of the cybersecurity system is thus paramount {21.03}. For example, the cybersecurity audit log integrity is important because attackers attempt to alter the log to hide evidence of their cyberattack activities.

*Implications.* The cybersecurity system must be carefully designed to itself be secure. The cybersecurity of the cybersecurity system cannot depend on any other less secure systems. Doing so creates an indirect avenue for attack. For example, if the identity and authentication process for access maintenance ports for updating the cybersecurity system use simple passwords over remotely accessible network ports, that becomes the weakest link of the entire system. In addition, cybersecurity engineers cannot simply use the cybersecurity mechanism that the cybersecurity system provides to protect the mission systems. In other words, the cybersecurity system cannot use itself to protect itself; that creates a circular dependency that will almost certainly create an exploitable flaw an attacker can use. Lastly, the cybersecurity mechanisms are usually hosted on operating systems and underlying hardware, which become the underbelly of the cybersecurity system. That underbelly must be secured using different cybersecurity mechanisms, and it is best if those mechanisms can be as simple as possible. Complexity is the

enemy of cybersecurity because of the difficulty of arguing that complex systems are correct {19.09}.

► **Depth without breadth is useless; breadth without depth, weak {08.02}.**

*Description.* Much ado has been made about the notion of the concept of *defense in depth*. The idea is often vaguely defined as layering cybersecurity approaches including people, diverse technology, and procedures to protect systems. Much more precision is needed for this concept to be truly useful to the cybersecurity design process. Layer how? With respect to what? The unspoken answer is the cyberattack space that covers the gamut of all possible attack classes as shown in the accompanying figure.

*Rationale.* One must achieve depth with respect to specified attack classes. Mechanisms that are useful against some attack classes are entirely useless against others. This focusing idea fosters an equally important companion principle: *defense in breadth*. If a cybersecurity designer creates excellent depth to the point of making a particular class of attack prohibitive to an adversary, the adversary may simply move to an alternative attack. Thus, *one must cover the breadth of the attack space, in depth*. Ideally, the depth will be such that all avenues

of attack, for all attack classes, will be equally difficult, and above the cost and risk thresholds of the attackers.

*Implications.* This depth-and-breadth principle implies that the cybersecurity engineer must have a firm understanding of the entire spectrum of cyberattacks, not just a few attacks. More broadly, the principle suggests the cybersecurity community must develop better cyberattack taxonomies that capture the entire attack space, including hardware attacks, device controller attacks, operating system attacks, and cyberattacks used to affect the beliefs of people. Further, the principle also means that cybersecurity measures must be properly characterized in terms of their effectiveness against the various portions of the cyberattack space. Those who create or advocate for various measures or solutions will be responsible for creating specific claims about their cyberattack-space coverage, and analysts will be responsible for designing tests to thoroughly evaluate the validity of those claims. Lastly, cybersecurity architects will need to develop techniques for weaving together cybersecurity in ways that create true depth, measured by how the layers alter the probability of success an adversary

will have for the targeted attack class. Said a different way, *the effectiveness of depth could be measured by how miserable it makes an attacker's life*.

► **Failing to plan for failure guarantees catastrophic failure {20.06}.**

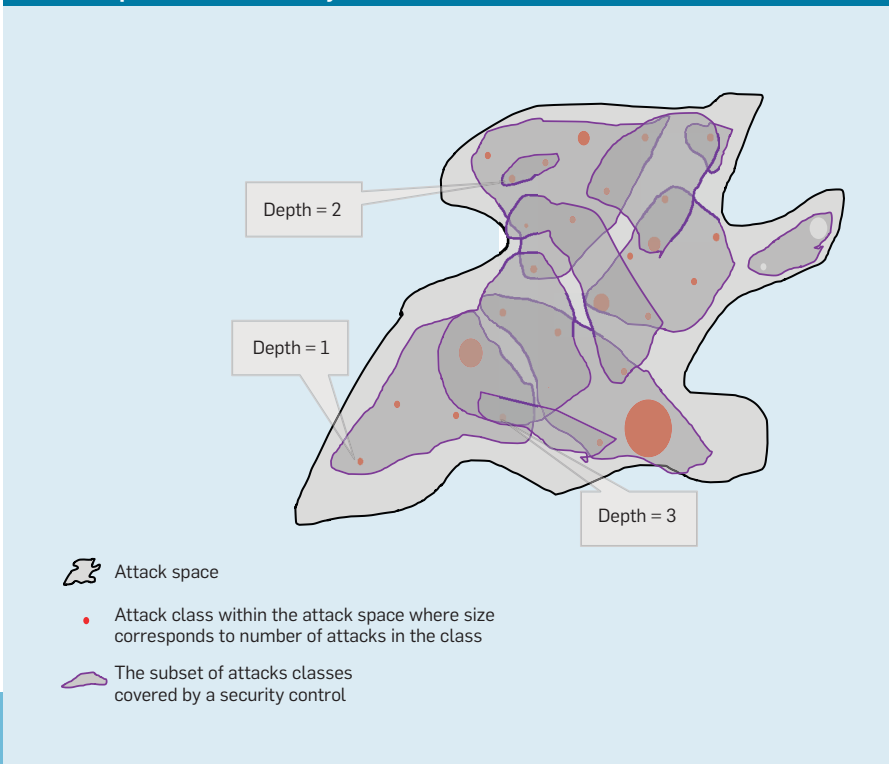
*Description.* System failures are inevitable {19.01, 19.05}. Pretending otherwise is almost always catastrophic. This principle applies to both the mission system and cybersecurity subsystem that protects the mission system. Cybersecurity engineers must understand that their systems, like all systems, are subject to failure. It is incumbent on those engineers to understand how their systems can possibly fail, including the failure of the underlying hardware and other systems on which they depend (forexample, the microprocessors, the internal system bus, the network, memory, and external storage systems). A student of cybersecurity is a student of failure {07.01} and thus a student of dependability as a closely related discipline. Security requires reliability; reliability requires security {05.09}.

*Rationale.* Too many cybersecurity engineers forget that cybersecurity mechanisms are not endowed with magical powers of nonfailure. Requirements can be ambiguous and poorly interpreted, designs can be flawed, and implementation errors are no less likely in security code than in other code. Indeed, security code often has to handle complex timing issues and sometimes needs to be involved in hardware control. This involves significantly more complexity than normal systems and thus requires even more attention to failure avoidance, detection, and recovery {05.10}. Yet the average cybersecurity engineer today seems inadequately schooled in this important related discipline.

*Implications.* Cybersecurity engineering requires design using dependability engineering principles. This means that cybersecurity engineers must understand the nature and cause of faults, how the activation of faults lead to errors, which can propagate and cause system failures.<sup>1</sup> They must understand this not only with respect to the cybersecurity system they design, but all the systems on which the system depends and which depend on it, including the mission system itself.

► **Strategy and tactics knowledge**

Defense depth and breadth in a cyberattack.



### comes from attack encounters {01.09}.

*Description.* As important as good cybersecurity design is, good cybersecurity operations is at least as important. Each cybersecurity mechanism is usually highly configurable with hundreds, thousands, and even millions of possible settings (for example, the rule set of firewalls denying or permitting each combination, port, protocol, source address range, and destination address range). What are the optimal settings of all of these various mechanisms? The answer depends on variations in the mission and variations in the system environment, including attack attempts that may be ongoing. The settings are part of a trade-off space for addressing the entire spectrum of attacks. The reality is there is no static optimal setting for all cyberattack scenarios under all possible conditions {22.07}. Furthermore, dynamically setting the controls leads to a complex control-feedback problem {23.11}. Where does the knowledge come from regarding how to set the security control parameters according to the particulars of the current situation? It is extracted from the information that comes from analyzing cyberattack encounters, both real and simulated, both those that happen to one's own organization and those that happen to one's neighbors.

*Rationale.* There is certainly good theory, such as game-theory based approaches,<sup>2</sup> which one can develop about how to control the system effectively (for example, using standard control theory). On the other hand, practical experience plays an important role in learning how to effectively defend a system. This knowledge is called strategy (establishing high-level goals in a variety of different situations) and tactics (establishing effective near-term responses to attack steps the adversary takes).

*Implications.* Strategy and tactics knowledge must be actively sought, collected with intention (through analyzing real encounters, performing controlled experiments, and performing simulations {23.04}), curated, and effectively employed in the operations of a system. Cybersecurity systems must be designed to store, communicate, and use this knowledge effectively in the course of real operations. Plans

based on this knowledge are sometimes called playbooks. They must be developed in advance of attacks {23.05} and must be broad enough {23.07} to handle a large variety of attack situations that are likely to occur in real-world operations. The process of thinking through responses to various cyberattack scenarios, in itself, is invaluable in the planning process {23.10}. Certain responses that may be contemplated during this process may need infrastructure (such as, actuators) to execute the action accurately and quickly enough {23.15} to be effective. This insight will likely lead to design requirements for implementing such actuators as the system is improved.

### The Future

Systematically extracting, presenting, and building the principles underlying trustworthy systems design is not the work of one cybersecurity engineer—not by a long shot. The task is difficult, daunting, complex, and never-ending. I mean here to present a beginning, not the last word on the matter. My goal is to encourage the formation of a community of cybersecurity and systems engineers strongly interested in maturing and advancing their discipline so that others may stand on their shoulders. This community is served by like-minded professionals sharing their thoughts, experiences, and results in papers, conferences, and over a beverage during informal gatherings. My book and this article are a call to action for this community to organize and work together toward the lofty goal of building the important underpinnings from a systems-engineering perspective.

Lastly, I will point out that cyberattack measures and cybersecurity countermeasures are in an eternal co-evolution and co-escalation {14.01}. Improvements to one discipline will inevitably create an evolutionary pressure on the other. This has at least two important implications. First, the need to build cybersecurity knowledge to build and operate trustworthy systems will need continuous and eternal vigilant attention. Second, communities on both sides need to be careful about where the co-evolution leads. Faster and faster cyberattacks will lead cybersecurity

defenders to autonomic action and planning that may eventually be driven by artificial intelligence. Stronger and stronger cybersecurity measures that dynamically adapt to cyberattacks will similarly lead adversaries to more intelligent and autonomic adaptations in their cyberattacks. The road inevitably leads to machine-controlled autonomic action-counteraction and machine-driven adaptation and evolution of mechanisms. This may have surprising and potentially disastrous results to the system called humanity {25.02, 25.04}.

### Acknowledgments

First and foremost, I acknowledge all of the formative conversations with my technical mentor, Brian Snow. He is a founding cybersecurity intellectual who has generously, gently, and wisely guided many minds throughout his illustrious career. Second, I thank the dozens of brilliant cybersecurity engineers and scientists with whom I have had the opportunity to work over the last three decades. Each has shone a light of insight from a different direction that helped me see the bigger picture of underlying principles. □

### References

1. Avizienis, A., Laprie, J.-C., and Randell, B. Fundamental concepts of dependability. In *Proceedings of the 3<sup>rd</sup> IEEE Information Survivability Workshop* (Boston, MA, Oct. 24–26). IEEE, 2000, 7–12.
2. Hamilton, S.N., Miller, W.L., Ott, A., and Saydjari, O.S. The role of game theory in information warfare. In *Proceedings of the 4<sup>th</sup> Information Survivability Workshop*. 2001.
3. Hammond, S.A. and Mayfield, A.B. *The Thin Book of Naming Elephants: How to Surface Undiscussables for Greater Organizational Success*. McGraw-Hill, New York, 2004, 290–292.
4. Morgan, S. *Top 5 Cybersecurity Facts, Figures and Statistics for 2018*. CSO Online; <https://bit.ly/2KG6jJV>.
5. NASA. *Report of the Presidential Commission on the Space Shuttle Challenger Accident*. June 6, 1986; <https://history.nasa.gov/rogersrep/genindex.htm>
6. Rand Corporation. *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*. Rand Corp. 2009; [https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND\\_MG654.pdf](https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf)
7. Saydjari, O.S. *Why Measure? Engineering Trustworthy Systems*. McGraw-Hill, New York, 2018, 290–292.
8. Saydjari, O.S. *Engineering Trustworthy Systems: Get Cybersecurity Design Right the First Time*. McGraw-Hill Education, 2018.
9. Wiegmann, D. and Shappell, S.A. *A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System*. Ashgate Publishing, 2003.
10. Zarate, J.C. The Cyber Attacks on Democracy. *The Catalyst* 8, (Fall 2017); <https://bit.ly/2IXttZr>

**O. Sami Saydjari** (ssaydjari@gmail.com) is Founder and President of the Cyber Defense Agency, Inc., Clarksville, MD, USA.

Copyright held by author/owner.  
Publication rights licensed to ACM. \$15.00.

Copyright of Communications of the ACM is the property of Association for Computing Machinery and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.