FEATURE

Analyst and Adversary

Deconstructing the "Imaginary" of Security and Cybersecurity Professionals

Do you have something to say about this article?

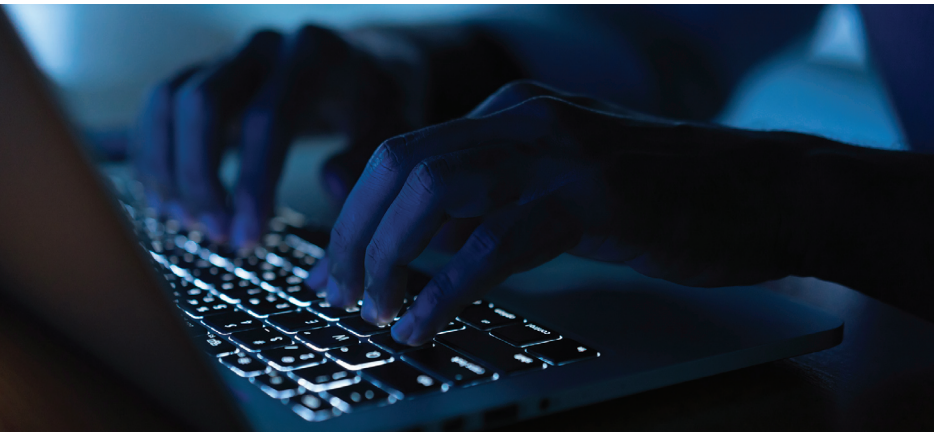
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2HIdw8H

Disponible también en español

Each year, reports of new threats and security breaches reveal the ever-increasing sophistication of attackers and their methods for outwitting available control mechanisms.[1,2] These developments reflect the evolution of an adversary who constantly strives to find novel, surprising attack vectors and create instability across the corporate private sector, as well as the military and governments at national, state and local levels.

Security and cybersecurity researchers attempt to study the mind-set of attackers—hoping to understand how they think, reflect, develop strategies and act. However, the field is generally characterized by conflicts and adverse conditions that few practitioners will find attractive; such research is inherently prone to overstepping ethical boundaries that security and cybersecurity specialists should respect when carrying out their professional duties.[3] In this context, the attacker becomes at once close and distant, occupying a zone of contradiction that prohibits any advancing beyond certain ethical limits on security and cybersecurity practice. Nonetheless, the study of adversaries and their attack methods forms an integral part of security and control practice—not only because attacks create the very instability that security professionals are dedicated to avoiding, but also because studying and emulating attacks, in controlled circumstances, can provide valuable insight to business and security leaders.



Many security analysts advance the professional vocabulary of threats, controls and impacts—that is, those on the light side of the force, so to speak—guided by ethics and adherence to regulations. Other so-called analysts allow themselves to be tempted by the dark side; however, recognizing potential vulnerabilities in practice, their intentions shift, and their capabilities become ambiguous. The contrast captures certain unavoidable tensions that arise in the security profession: tension between the necessity to take chances and understand the adversary, on the one hand, and risk aversion and the duty to avoid exposure, on the other hand; and tension between a mandate to achieve greater reliability vs. an attitude of healthy skepticism and imperfect trust[4,5] in a world that is ever more hyperconnected, digitally transformed—and, therefore, exploitable.

Certain conceptual foundations have remained constant throughout the training and practice of security and cybersecurity professionals—foundations informing what might be called their professional imaginary—that is, a certain inherited perspective, received wisdom or set of assumptions projected outward on a rapidly evolving world. Comprehending and analyzing the security imaginary can open a space for new options and alternative considerations, making it possible to reconstruct and validate previous knowledge and experience, better protect and secure organizations while advancing their digital strategies, and also spark new debates on the way to defend and preempt attacks in today's asymmetrical and uncertain world.

Jeimy J. Cano M., Ph.D., Ed.D., CFE, CICA
Is professor at the school of law of the Universidad de los Andes, Colombia. He has more than 22 years of experience as an executive, academic and professional in the areas of information security, cybersecurity, forensic computing, digital crime, critical infrastructures and IT auditing.

Education and Training: Forming the Professional Imaginary

Constant change and adaption to the challenges of the world increasingly require workers to become life-long students.[6] The traditional model of education in which professors possess knowledge and students passively receive and store their teaching tends to reproduce a homogeneous educational status quo; one that is becoming steadily less relevant. In such circumstances, students often essentially repeat or confirm the accomplishments of their mentors in order to obtain the highest grades, awards and recognition from the institutions at which they study. This educational model tends to assume—if not also re-create—a mechanistic society in which it is possible to forecast the behavior of the system and its participants. It presupposes a context for work and learning that treats all learners identically, frequently ignoring any prior knowledge or individual characteristics, and molding their vision of the world according to currently accepted standards—all in order to address issues or challenges with solutions already known to the educators.

> “THE DIGITAL ADVERSARY FEELS COMFORTABLE WITH UNCERTAINTY AND INSTABILITY, IS NOT AFRAID TO BE WRONG AND, IN EACH OUTCOME, FINDS AN OPPORTUNITY TO CAPITALIZE AND UPDATE KNOWLEDGE.”

Education in security and cybersecurity was formed in this mold. Its frameworks and approaches to learning are all but unquestionable and dictate how security specialists learn to make decisions. Aversion to risk, a need to control actions and consequences, and fear of failure perceived as inevitable condition the ways that security practitioners respond in the face of a reality that is utterly different from the one which formed their training—one that demands a different perspective to recognize and understand new risk scenarios and emerging threats. Current professional frameworks in both security and cybersecurity seek to create certainties and a feeling of control with the understanding that, as good practices, the frameworks are sufficient to affect reality and preempt acts by adversaries. Standard practices that currently inform the imaginary of security and cybersecurity professionals must not become dogmas and unquestionable truths; rather, they should be subject to review and analysis, constantly reevaluated in the context of emerging professional experience and organizational dynamics.

Professionals responsible for security must break away from the paradigm of known controls and allow themselves to be questioned and interrogated by the volatile, uncertain, complex and ambiguous experience of working in the field; in effect, they need to uninstall the responses programmed and validated by their education and applied within their working contexts. They must invent alternatives that are not simple reactions to unexpected events but, instead, make it possible to anticipate, defend and preempt the adversary’s moves, connecting the disconnected dots in their environments and creating an enriched vision for their recommendations and actions. Practitioners must remember that an analyst’s success poses a new challenge to an adversary, i.e., an increase of the attacker’s creativity to add tension to the new security and control policies.

The Digital Adversary and the Capacity to Surprise

To protect and advance the value promise of the enterprise, security and cybersecurity specialists seek to implement, secure, stabilize and protect assets under their care. All the while, their adversary is continually preoccupied with experimenting, surprising, destabilizing and compromising (that is, breaching or outwitting known standards and protections), naturally creating instability and spreading uncertainty.

The digital adversary feels comfortable with uncertainty and instability, is not afraid to be wrong, and, in each outcome, finds an opportunity to capitalize and update knowledge. The digital adversary accelerates learning, as well as constructive unlearning, through permanent testing

Enjoying this article?

- Read *Threat Intelligence. www.isaca.org/threat-intelligence*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA’s Online Forums. *https://engage.isaca.org/onlineforums*

and experimentation and pursues or re-creates contexts that, for others, may feel uncontrolled—all with the goal of reaching new frontiers of knowledge that customary security practices and science have (so far) not attained. This mode of thinking and acting emphasizes the development of critical capacity and an ongoing strategy to supersede known truths and conventional wisdom. The adversary exposes the *status quo* to new test cases to find new opportunities, uncover conditions that lead to novel approaches and take the most advanced digital protections by surprise. To understand what happened in the case of a breach, security professionals often head down a road that adversaries have already traveled.

The attacker understands security not as a final objective to achieve, but as an incomplete journey; preliminary and partial responses are the norm, vulnerabilities require adaptive goals, and security demands lead to imperfect trust. The adversary's mind is restless; either it was never formed within the mentality and framework of traditional education, or it quickly outgrew them. Instead, the adversary responds to the adrenaline rush produced by breaking existing protection paradigms. He or she relishes a sense of permanent inevitability of security failure as the new normal in the education of security and control specialists.

> "UNDERSTANDING THE MIND OF THE ADVERSARY CAN OPEN SPACE FOR THE AUTHENTICALLY ENLIGHTENED TRAINING OF THE SECURITY AND CONTROL PROFESSIONALS."

Yet, understanding the mind of the adversary can open space for the authentically enlightened training of the security and control professionals. It can teach them to understand the instability of the present, the possibilities open in a hyperconnected world and, above all, a systemic rationale that is not based on fixed or mechanistic causality or an immutable reality governed by known laws but rather one that is relational and emerging; is capable of unifying vision in the midst of oddities, inconsistencies and contradictions;[7] creates synthesis between reality and imagination; transforms uncertainty into opportunity; creates incentives; ruptures the *status quo*; and reveals what was heretofore impossible to see. Practitioners should remember that an adversary's success represents a lesson learned to an analyst, i.e., new motivations for the analyst to explore and challenge previous knowledge.

Analyst and Adversary: Integrating Two Opposing Visions

Finding value in the methodology of adversaries is not intended to romanticize or promote illegal activity. Rather, it illustrates how their methods, mind-set and culture can be repurposed to enrich the education and training of security and cybersecurity professionals. The old, static practices around controls (and their respective verifications) will not be viable for 21st century organizations as a source of imperfect trust. In fact, improving security and cybersecurity today will depend on consciously and selectively integrating these historically opposing roles.

The analyst conventionally works across three categories: threat, control and impact (i.e., a common vocabulary, widely recognized and accepted across enterprises). The adversary thinks in terms of intention, capacity and vulnerability (**figure 1**). The categories of the analyst generally entail negative reactions to the open-ended, dynamic terms of the adversary. The analyst closes off (or at least reduces) attack surfaces; the adversary emphasizes possibility, openness and opportunity. Harmonizing these oppositions may seem contradictory or counterintuitive, but for the analyst, actually encourages a constructive unlearning of existing assumptions and tactics that may be inherently weak by virtue of their standardization and ubiquity (i.e., their status as best practice).

Figure 1—Analyst and Adversary: Integrating Two Opposing Visions

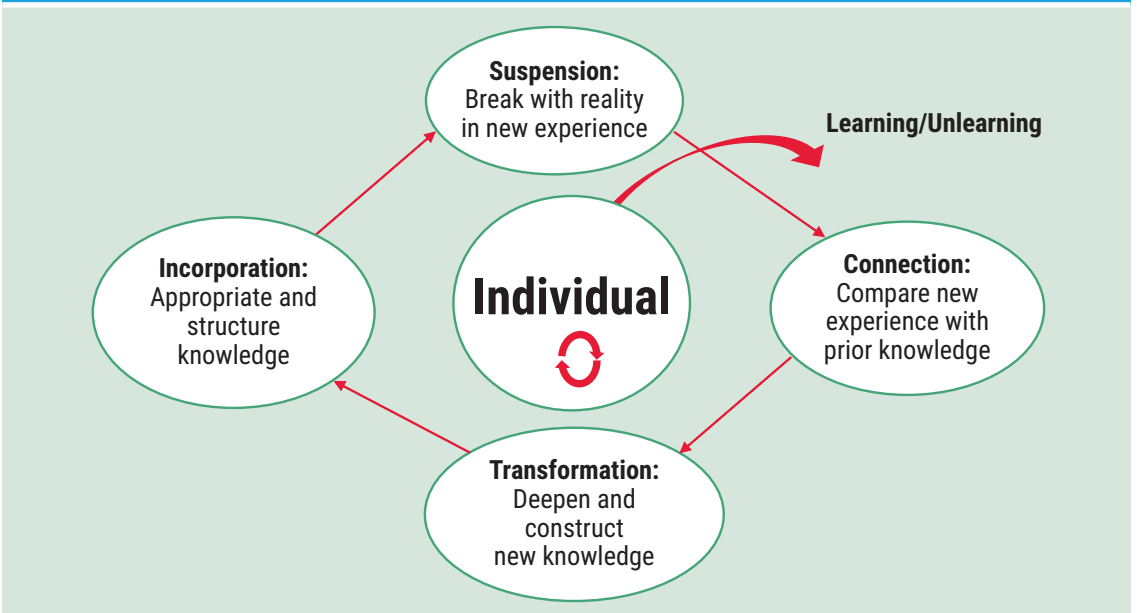
	Actors		
	Analyst	**Adversary**	
Mechanical view: Linear	Threat	Intention	Relational view: Circular
	Control	Capacity	
	Impact	Vulnerability	
Stance: Implement, secure and protect	<--OPPOSING VISIONS-->		Stance: Experiment, surprise and compromise

Figure 1 offers a pedagogical model to harmonize opposing visions. It graphically invites the analyst to supplement defensive postures with the more offensive outlook and behavior of the adversary. The model intentionally escapes the analyst's psychological safe zone,[8] invites decisions in the face of uncertain conditions, and creates new opportunity for analysts to "study the situation, define the problems, come to their own conclusions about the actions to undertake, compare ideas, defend them and rework them with new contributions."[9]

Concretely, the new pedagogy rests on four stages for transforming learning and incorporating constructive unlearning (**figure 2**):

- **Suspension**—Conditioned by existing knowledge, reality is challenged or contradicted by new experience, which disrupts the inertia of current, accumulated wisdom. This break, a rupture in what formerly was considered "real" or true, requires existing practice to be questioned and encourages the analyst to identify aspects of the situation that are unknown, unresolved or undefined, relative to current standards and/or contexts. Uncertainty creates tension in prior knowledge.
- **Connection**—Novel experience is associated with previous experience; comparisons are made and interrogated or tested in light of prior knowledge. Trial and error are grasped as a process, creating

Figure 2—The Learning and Unlearning Process



Source: Adapted from Reyes, A.; R. Zarama; "The Process of Embodying Distinctions: A Reconstruction of the Process of Learning," Cybernetics and Human Knowing, vol. 5, no. 3, 1 March 1998, *https://www.ingentaconnect.com/contentone/imp/chk/1998/00000005/00000003/14*. Reprinted with permission.

opportunities to learn and assimilate skills that gradually become proven practice. Successful resolution of prior conflicts or difficulty is evaluated as a basis for action in similar situations.

- **Transformation**—Uncertainty gradually yields to the construction of new knowledge. Known elements of practice, including current concepts regarding threat and risk, are superseded and discarded. New distinctions and categories lead to an emerging hypothesis that responds to—or accounts for—the anomalies, contradictions or discontinuities of the new experience.
- **Incorporation**—A new information structure is built from previous knowledge, codified and disseminated. It incorporates new interpretations and a renewed awareness of fragility and asymmetry in the security field. While acknowledging the inevitability of failure, the analyst gains new perspectives on the practical benefit of safeguarding the enterprise's value promise, which later assumes new urgency and validity. The analyst's responsibility and purpose appear more evident, especially in uncertain situations.

Rethinking education according to these principles requires breaking with the current mechanistic tradition, whose standards demand routine, repeatable processes to measure levels of protection—whether actual or aspirational—for the organization. The goal is to complement or expand current approaches, privilege openness, anticipate the actions of adversaries (and assess consequences), tolerate calculated risk, emphasize initiative and experimentation, and revise or update knowledge now and in the long term.[10]

Conclusions

As risk and emerging threats increase—along with legal requirements for compliance[11]—the mechanistic education of information security and cybersecurity analysts reveals its inherent limitations. Current approaches to security and control should become more forecasting and preemptive, expanding the current educational framework, which generally ensures good practices that create certainties and calmness in decision-making. Forecasting means recognizing, confronting, learning and unlearning, engaging the uncertainty and instability of emerging risk, internalizing the adversary's mind-set, and updating prior knowledge—and its conceptual foundation—to include elements of experimentation, surprise and even amazement.[12]

Security and control managers should be less afraid that they will "lose sight of the shore" of conventional standards and good practices and, instead, commit themselves to reinventing knowledge on the basis of present capacities and demands. Although security managers will never have everything they need to succeed in all circumstances, they do have the ability to learn and unlearn and, thus, to envision what they want to achieve, to construct forecasts, and understand that incidents are a natural part of the landscape for modern organizations.

"THE MECHANISTIC EDUCATION OF INFORMATION SECURITY AND CYBERSECURITY ANALYSTS REVEALS ITS INHERENT LIMITATIONS."

Analysts and adversaries share a foundation of knowledge and common challenges. Analysts should adopt the adversary's tools wherever it makes sense; leave their comfort zones; explore different points of view (perhaps even from other disciplines or intellectual positions); develop habits, attitudes, capacities and meanings to overcome cognitive blindness;[13] act preemptively; and, especially, stay ahead of the curve: preempt, challenge, interpret, decide, (re)align and learn.

Endnotes

1 Accenture, *The Post-Digital Era Is Upon Us: Are You Ready for What's Next?* Accenture Technology Vision 2019, *https://www.accenture.com/t20190201T224653Z__w__/us-en/_acnmedia/PDF-94/Accenture-TechVision-2019-Tech-Trends-Report.pdf*

2 European Union Agency for Network and Information Security (ENISA), *ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends*, January 2019, *https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport*

3 Do, Q.; B. Martini; K. R. Choo; "The Role of the Adversary Model in Applied Security Research," *Computers & Security*, vol. 81, March 2019, *https://eprint.iacr.org/2018/1189.pdf*

4 In a hyperconnected world, all participants are going to have some kind of failure and need to act when this happens. Reliability is based on the impact of adverse actions and how to manage them.

5 Cano, J.; "Riesgo y seguridad. Un continuo de confianza imperfecta," in Dams, A.; H. Pagola; L. Sánchez; J. Ramio; *Actas IX Congreso Iberoamericano de Seguridad de la Información*, Universidad de Buenos Aires–Universidad Politécnica de Madrid, 2017, p. 34-39, *https://www.researchgate.net/publication/321197873_Riesgo_y_seguridad_Un_continuo_de_confianza_imperfecta*

6 For example, two researchers note, "One of the most urgent challenges facing higher education is how to respond to the unavoidable need to modernize and improve the competencies of an ever-greater number of people throughout both the length and breadth of their lives." Echeverría, B.; P. Martínez; "Revolución 4.0, Competencias, Educación y Orientación," *Revista Digital de Investigación en Docencia Universitaria* 12:2, *http://dx.doi.org/10.19083/ridu.2018.831*

7 Charan, R.; *The Attacker's Advantage: Turning Uncertainty Into Breakthrough Opportunities*, Public Affairs, USA, 2015, *https://www.publicaffairsbooks.com/titles/ram-charan/the-attackers-advantage/9781610394758/*

8 The psychological safe zone is clearly understandable reactions to the interests and mandates of senior security and cybersecurity management. See Edmondson, A.; *The Fearless Organization: Creating Psychological Safety in the Workplace for Learning, Innovation, and Growth*, John Wiley & Sons, USA, 2018, *https://www.wiley.com/en-us/The+Fearless+Organization:+Creating+Psychological+Safety+in+the+Workplace+for+Learning,+Innovation,+and+Growth-p-9781119477266*

9 Acosta, S.; *Pedagogía por competencias: Aprender a pensar*, Editorial Trillas, Mexico, 2012, p. 47, *www.etrillas.com.mx/detalle.php?isbn=9786071713025&estilo=13&tema=0*

10 Cano, J.; "La educación en seguridad de la información. Reflexión pedagógicas desde el pensamiento de sistemas," *Memorias 3er Simposio Internacional en "Temas y problemas de Investigación en Educación: Complejidad y Escenarios para la Paz,"* 2016, *http://soda.ustadistancia.edu.co/enlinea/congreso/congresoedu/2%20Pedagogia%20y%20dida%B4ctica/2%209%20LA%20EDUCACION%20EN%20SEGURIDAD%20DE%20LA%20INFORMACION.pdf*

11 IT Governance, "Managing Cyber Risk: Transform Your Security With Cyber Resilience," *https://www.itgovernance.co.uk/managing-cyber-risk*

12 One author celebrates the quality of amazement in discovering what lies concealed behind everyday experience—of perceiving, for the first time, what has been there all along. See García, A.; *Educar para el asombro. Sencillez, confianza, paciencia y profundidad*, Mensajero, Spain, 2018, *https://gcloyola.com/es/educacion/3139-educar-para-el-asombro-9788427141759.html?search_query=educar+para+el+asombro&results=302&, p. 116.*

13 Krupp, S.; P. Schoemaker; *Winning the Long Game: How Strategic Leaders Shape the Future*, Public Affairs, USA, 2014, *https://www.publicaffairsbooks.com/titles/steven-krupp/winning-the-long-game/9781610394475/*