Advanced Sciences and Technologies for Security Applications

Carl S. Young

Cybercomplexity

A Macroscopic View of Cybersecurity Risk

Springer

Advanced Sciences and Technologies for Security Applications

Indexed by SCOPUS

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

Carl S. Young

Cybercomplexity

A Macroscopic View of Cybersecurity Risk

Springer

Carl S. Young
New York, NY, USA

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-031-06993-2 ISBN 978-3-031-06994-9 (eBook)
https://doi.org/10.1007/978-3-031-06994-9

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Only entropy comes easy.
Anton Chekov

To Geraldine Prose Young, MD
September 30, 1926–June 14, 2020

Foreword

In 1996, I was selected to start one of the first "Computer Crime Squads" in the New York office of the FBI. At that time, the Internet was starting to become a common utility, where access was facilitated by dial-up connections from telephone landlines.

As an investigative agency, the focus of the FBI was to understand how the Internet would affect investigations and what evidence would be available whenever this new medium was utilized. As I jumped into what was then a new and fast-growing field, other experienced FBI agents told me the one person with whom I should consult was Carl Young.

In those days, Carl was heading a unit within the Engineering Research Facility at the FBI Academy in Quantico, VA. I scheduled a meeting with Carl in his office, and during our discussion, it became clear why I was directed to speak to this individual.

Carl eventually became a member of the Senior Executive Service within the FBI Intelligence Division. Despite his senior status, Carl sought to understand "ground truth" by listening to the operational requirements of fellow investigators. He leveraged his education in physics to solve problems that had a significant impact on national security. He possessed a rare combination of operational experience, academic training, and facility for problem solving, and his input was valued by executive management, scientists, and FBI agents in the field alike.

That initial meeting marked the beginning of a relationship that has continued for over 20 years. Carl and I retired from the FBI in 2000, and each of us transitioned to the private sector. Carl joined Goldman Sachs in New York and I founded Stroz Friedberg, LLC, one of the first computer forensic firms.

We continued to discuss cybersecurity risk, his experiences at Goldman, and my experience working hundreds of engagements for clients and ultimately coalesced into a shared vision of what was needed in the marketplace. I invited Carl to join my firm and he did, launching what he aptly called the "Security Science" division.

We were immediately able to draw from a unique set of experiences and internal case studies our company owned. Those studies enabled us to review "postmortems" in an attempt to identify areas of commonality. We repeatedly observed the same types of issues across organizations and agreed their root cause was viewing cybersecurity

as an exclusively technical issue. This realization continues to influence our thinking on cybersecurity risk management.

In Carl's fifth reference book on security risk management, *Cybercomplexity*, he addresses one of the most challenging issues in cybersecurity. He does so by leveraging elementary probability and information theory to develop a simple model of complexity in IT environments while drawing on analogies from physical science. He also reveals why specific types of security controls are required to reduce complexity and thereby address cybersecurity risk on an enterprise scale.

Cybercomplexity does not indulge in technical jargon or "acronymology" and is therefore accessible to non-scientists. It represents another example of this author's success in applying science to security and is a reaffirmation of the close connection between the two areas. I have heard Carl say he hopes he can at least modestly improve the "signal-to-noise ratio" of security risk management. This book has clearly done that and more.

For any individual wishing to understand the foundations of cybersecurity risk, this book offers a resource to be repeatedly consulted. It offers unique insights into issues that affect all IT environments and that have confounded cybersecurity professionals for years. Importantly, it can enhance the sophistication of reporting to senior executives and boards of directors with respect to cybersecurity risk management challenges and best practices.

The level of success we achieve in cybersecurity is greatly affected by how we get to the core of its problems. By embracing this book's lessons, practitioners, managers, and executives will promote a security culture that reflects the thoughtfulness of a scientific approach.

Edward M. Stroz
Founder, Stroz Friedberg LLC
New York, NY, USA

Preface

What does "cybersecurity" actually mean? A book's title should reflect its content as a matter of principle if not professional courtesy. Specifically, is the use of "cyber" appropriate in this context noting the term is already a fixture in the English vernacular? To answer this question, it is helpful to explain its origins.

The first use of the term cyber was in Norbert Weiner's famous work, *Cybernetics*.[1] It derived from the Greek word *kubernetes* or "steersman" and has the same root as the English word "governor" as in the controller or speed limiter of a machine. The term cybernetics is a reference to the confluence of communication and control, which is the central theme of *Cybernetics*.[2] Weiner, a professor of mathematics at the Massachusetts Institute of Technology, coined the term in 1948.

Weiner recognized that "the problems of communication and control engineering were inseparable."[3] For example, the otherwise pedestrian task of eating with a fork is less appreciated as a problem in communication and control. The brain is iteratively processing positional data while updating the signals transmitted to the muscles that guide the fork to its destination. When viewed in this light, shooting down a missile and eating with a dining utensil are each exercises in optimal prediction.

Weiner made the profound revelation that the central focus in addressing such problems should be the signal message, which is characterized as "a discrete or continuous sequence of measurable events distributed in time."[4] Statisticians refer to these sequences as *time series*.

Moreover, he reasoned the solution to problems in optimal prediction could be found in time series statistics, and more specifically, in finding an explicit expression for the so-called mean square error of prediction. The presence of background noise

---

[1] N. Weiner, Cybernetics; Or Control and Communication in the Animal and the Machine; MIT Press, John Wiley and Sons, New York, NY, 1948.

[2] A. Broadhurst and D. Darnell, An Introduction to Cybernetics and Information Theory, *Quarterly Journal of Speech*, Volume 51, 1965.

[3] N. Weiner, op. cit. 1948.

[4] Ibid.

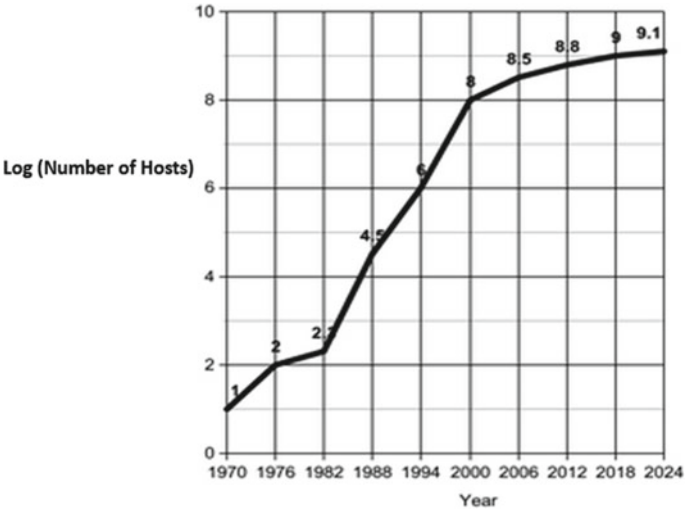

Fig. 1 Internet usage by year

is the complicating feature, and recovering the transmitted message depends on the statistical nature of the message and the corrupting noise.

Weiner notably posited that humans and machines were equivalent with respect to communication when viewed through a cybernetic lens. In that vein, cybernetics and cybersecurity share a common theme in that the predicate for both disciplines derives from machines as communication devices.

This thematic connection is particularly significant in light of the ascent of computer technology in communication. These days, computers (broadly defined) are integral to most forms of communication, and reliable access to the Internet has become a necessity.

To gain some perspective, Google alone processes more than 40,000 searches *per second*.[5] One 2021 estimate of the number of Internet-connected devices is 27.1 billion.[6] Figure 1 illustrates the explosive adoption of the Internet as a means of communication, noting the vertical axis is a logarithmic scale.[7]

Although Weiner was among the first to recognize the inherent relationship between machines and communication, even he might not have anticipated the rapid evolution of modern computing. The ubiquitous presence of information technology is in part a result of improvements in electronic storage, channel capacity, and connectivity. Techniques for mass production have also evolved so that information technology is accessible to broad segments of the population.

[5] www.forbes.com; May 21, 2018.

[6] www.cisco.com.

[7] Internet Count History, Internet Systems Consortium.

However, machines and humans perhaps have an even deeper relationship through the numerous applications that can be downloaded via the Internet. Nowadays, individuals possess a digital identity defined by these applications. Furthermore, digital identities are arguably displacing physical identities as online activities increasingly substitute for personal interactions. The COVID-19 pandemic might have accelerated this phenomenon, but continued virtualization is inevitable.

Cybersecurity is clearly affected by the trajectory of information technology and its usage. However, although the physical and virtual worlds increasingly overlap, they remain distinct in significant ways. For example, the methods used to restrict physical access, e.g., sensory perception, locks, physical barriers, and alarms, are not applicable to the virtual world. Less intuitive methods must be deployed to restrict electronic access. This problem is compounded by the perpetual desire for convenience, which has potentially disastrous consequences when sharing information online.

Increased computational power as predicted by Moore's Law resulted in miniaturization that has accelerated the dependence on information sharing.[8] Mobile devices and the accompanying fluidity of network boundaries have ramped up expectations of convenience while amplifying the need for cybersecurity. Smart phones, tablets, etc., enable unprecedented access to information irrespective of physical location.

In fact, the very notion of a physical boundary has become increasingly fuzzy in the virtual world. In many scenarios, it is downright meaningless. Network boundaries can be generously described as fluid, where Wi-Fi and cellular technologies extend the perimeter to anywhere within range of a radiating access point or cell tower. Convenience on that scale is inevitably accompanied by an increased potential for information compromise.

Note the nature of electronic information itself has security implications. Specifically, although information might have been stolen, it might not actually be missing. In other words, physical access to an item of value is not required in order to steal it.

One strongly suspects something is awry with respect to traditional approaches to cybersecurity risk management given the legacy of successful cyberattacks. Such attacks persist despite countless regulatory requirements, security policies, security technology standards, and sophisticated security technologies. Significantly, data breach *postmortems* frequently point to the same *modus operandi*.

One plausible explanation for the current situation is cybersecurity continues to be viewed as a technical issue rather than as a traditional problem in risk management. Therefore, the focus is on technology fixes simply because technology facilitates information exchange. The fact is that the root causes of cybersecurity risk often have nothing to do with technology.

According to cybernetics, man and machine are similar in how they process information. In cybersecurity, it is the interaction between man and machine that is most significant. To be clear, networked computers do precisely what they are designed to do: enable information sharing. Unfortunately, information security and information

[8] Moore's Law, named after Gordon Moore, CEO and co-founder of Intel, states that the number of transistors in an integrated circuit doubles every two years.

sharing are inherently in tension, which explains why cybersecurity professionals perpetually face an uphill battle.

At the risk of stating the obvious, cybersecurity would be much less challenging without the Internet. Bad things can occur when billions of invisible individuals exchange information via a highly distributed and massively convenient network. But Internet access is synonymous with easy information sharing, which is now integral to our personal and professional lives.

The Internet differs from other electronic networks in that the network nodes need not be physically connected. This property also has significant security implications. Most notably, it frees both authorized network users and miscreant network attackers from being constrained to specific physical locations.

Consider the telephone network before the days of IP telephony. Previous technology limited the power and flexibility of POTS devices but also reduced the potential for information compromise because physical access to the equipment was required.

I recall my university's more mischievous students perpetrating hacks against "Ma Bell" as the phone company was affectionately called. They were forced to physically access the equipment in order to commit their prank and thereby thumb their noses at "The Establishment," which the phone company personified in the nineteen seventies.

Modern hackers are both ethically less benign and physically less constrained than their forebears. Nowadays, a telephone is merely another device on the IP network, and therefore, hackers need not leave the comfort of their homes to wreak havoc on organizations and individuals alike.

There are other aspects of electronic networks that affect the security risk profile. Network communicators are invisible, and messages can be routed to their destination without attribution. Malicious actors exploiting technology vulnerabilities and/or human foibles drive the requirement for a strategy of "zero trust" when attempting to access information assets.

In the end, cybersecurity is about securing electronic information that is processed by machines, operated by humans, and connected via networks. These networks are vast in scope, opaque in detail, and highly diversified. The result is a multifaceted environment that enables unprecedented information sharing but is also ripe for exploitation. The proliferation of vulnerabilities in such environments is almost inevitable.

Security risk assessment outcomes are affected by how one addresses such vulnerabilities, and high-severity examples clearly require addressing in a timely manner. However, the aggregate effect of risk factors also impacts the potential for information compromise that includes non-technical issues associated with processes and workflows. Such effects are generally not visible unless IT environments are viewed through a sufficiently broad lens.

To that end, this text explores the *macroscopic* forces that affect IT environments on an enterprise scale and the implications to cybersecurity risk management. Specifically, *Cybercomplexity* is divided into four parts: (1) Security Risk Fundamentals, (2) Stochastic Security Risk Management, (3) Enterprise Cybersecurity Risk, and

(4) Cybercomplexity Genesis and Management. The following paragraphs describe the individual chapters within each of these sections.

Chapter 1, "Core Concepts," discusses the conceptual foundations of security risk and risk assessments. Although many readers may already be familiar with many of these concepts, thinking rigorously about risk requires a grasp of the basics, starting with the definitions of threat and risk.

Chapter 2, "Representing Cybersecurity Risk," focuses on the representation of risk-relevant phenomena. The objective is to explain concepts essential to understanding and conveying risk-relevant information.

Chapter 3, "Scale and Scaling Relations," represents a continuation of Chap. 2, where the focus is on describing relationships between risk-relevant parameters. A key result of the theory of complexity in IT environments is that the perspective or "scale" used to assess cybersecurity risk affects the assessment results. In particular, the existence of linear versus nonlinear scaling relations can have significant operational implications.

Chapter 4 is entitled "IT Environment Dimensions and Risk Factors." It describes a multi-dimensional representation of IT environments. These dimensions encompass the sources of risk factors for information compromise. The number of risk factors across all dimensions impacts cybersecurity risk on an enterprise scale and drives the requirement for a macroscopic approach to cybersecurity risk management.

Chapter 5, "Security Risk Management Statistics," begins the second section of the text. This chapter provides the conceptual foundations for a statistical description of IT environments. This description requires genericizing risk factors and security controls, where risk factors are either managed or not according to a binomial probability distribution. The result is IT environment states consisting of unique combinations of managed and unmanaged risk factors, thereby paving the way for applying the information theoretic formalism that follows next.

"Information Entropy" is the title of Chap. 6. Entropy is a concept derived from information theory, and it is fundamental to the model of complexity in IT environments. Specifically, information or Shannon entropy quantifies the uncertainty of a probability distribution, and it is the probability distribution of security risk management outcomes that leads to an expression for the unpredictability of IT environment states introduced in Chap. 5.

Chapter 7, "Complexity and Cybercomplexity," begins the third section of the text, which is entitled, "Enterprise Cybersecurity Risk." This chapter defines the general notion of complexity in terms of unpredictability and applies a binary stochastic security risk management model to IT environments. The result is a scaling relation for IT environment complexity in terms of the number of probable states of managed and unmanaged risk factors. The unpredictability of those states describes complexity in this context.

Chapter 8, "Cybercomplexity Metrics," specifies metrics that arise from a stochastic security risk management process. Although these metrics do not enable security control calibration, they represent a first step toward quantifying the effects

of complexity in IT environments. Perhaps more significantly, they highlight the relevance of scale in assessing cybersecurity risk as well as substantiate the requirement for the macroscopic security controls discussed in Chap. 10.

Chapter 9 "Cybercomplexity Root Causes," begins the final section of the text, "Cybercomplexity Genesis and Management." This section identifies the origins of complexity in IT environments and specifies requirements for its management. Chapter 9 delineates the most prominent root causes of Cybercomplexity, which are the progenitors of many cybersecurity incidents. This chapter is arguably the most operationally consequential in this section. Identifying and addressing the root causes of Cybercomplexity are necessary in reducing the potential for information compromise.

Chapter 10 "Macroscopic Security Controls," specifies the security controls that have a systemic effect on cybersecurity risk management. As their name implies, these controls function macroscopically, i.e., on an enterprise scale, and are antidotes to the root causes identified in Chap. 9.

Chapter 11 "Trust and Identity Authentication," focuses on trust in identity authentication, which is an issue that is currently top-of-mind in cybersecurity risk management. The concept of "zero trust" is particularly in focus. This chapter discusses how trust in identity can be formalized via a stochastic formulation of identity authentication.

Chapter 12, "Operational Implications," is the final chapter of the book. As its name implies, it focuses on the operational implications of cybercomplexity. Although such implications have been identified throughout the book, this chapter discusses the key implications in more detail as well as presents them in one place for reference. Candidly, these implications are mostly common sense and fortunately tend to confirm intuition about cybersecurity risk. Nevertheless, common sense is not necessarily common, and the implications can both inform and enhance traditional assessments of cybersecurity risk.

Finally, the principal focus of *Cybercomplexity* is on characterizing cybersecurity risk on an enterprise scale. The Cybercomplexity model is admittedly based on an idealized form of cybersecurity risk management. The contention is a probabilistic approach is helpful if not required to simplify IT environments and thereby examine cybersecurity risk at the desired scale.

The breadth and variability of IT environments have historically undermined such efforts. The intent is to overcome these obstacles by making simplifying assumptions in the hope of generalizing the results to more realistic scenarios. The good news is the lessons so derived make sense, and their broader applicability seems reasonable if not compelling.

New York, USA Carl S. Young

Acknowledgements

Writing acknowledgments can be challenging since the correlation between past contributions and present achievements is not always clear. Fortunately, the contributions of each individual mentioned below are timeless, which has made writing this particular acknowledgment especially easy.

My late parents, Dr. Irving Young and Dr. Geraldine Prose Young, have contributed significantly to everything I have achieved. Their enthusiastic support for their offspring has inspired family members across generations. My sisters, Diane Uniman and Nancy Young, continue the tradition by demonstrating love for me and support for my work.

Certain family friends deserve special mention due to the longevity and intensity of our friendship. Bill Seltzer, Vivian Seltzer, and Sora Landes have been like parents to me. Fortunately for them they have been spared that unenviable burden. I am grateful for their ongoing encouragement on this particular project as well the love they have shown me and my family over many decades.

I am fortunate to be close to a number of childhood friends who are still a key part of my life. These friends include Fran Davis, Maggie Degasperi, Dave Maass, Lisa Maass, Peter Rocheleau, Ruth Steinberg, and Jim Weinstein. The duration of these relationships exceeds 300 person-years, which is a testament to each individual's endurance and genuine affection.

I would be remiss if I did not mention the New Yorkers who are as close in spirit as they are in proximity. They include Maurice Edelson, Dick Garwin, Bob Grubert, Mal Ruderman, Paula Ruderman, and my cousin, Kate Smith. Donna Gill, collaborative pianist and vocal coach extraordinaire, deserves special mention, recalling our times together on the Upper West Side of Manhattan and *both* porches of her apartment in Chautauqua, NY.

Ed Stroz, the founder of Stroz Friedberg LLC, and more recently my partner in Consilience 360, has been a close friend and ally since I moved to New York City in 2000. His pioneering efforts in computer forensics have been influential in the evolution of computer security as well as my own thinking on that topic.

Steve Doty, the founder of Defensible Technology, is a friend, colleague, and a fellow advocate for risk-based security. It is rare to find a cybersecurity practitioner

who can reason about risk from first principles as well as design a secure network. Our numerous discussions on cybersecurity risk management have helped me bridge the gap between theory and practice.

As a professional statistical mechanic, Chris Briscoe possesses a physicist's understanding of both forms of entropy. Our discussions have been invaluable in helping me appreciate both the benefits and limitations of a probabilistic approach to security risk management.

Finally, I must acknowledge and thank my colleagues in the IT Department at The Juilliard School, with whom I have had the privilege of working since 2016. I have not worked with a more competent and dedicated group of technology professionals. My pride in their accomplishments in a challenging environment is only exceeded by my gratitude for all they have taught me.

New York, NY, USA Carl S. Young

Introduction

Cybersecurity professionals manage the risks associated with the threat of information compromise and information-related business disruption. The simplicity of their job description belies the difficulty of their job. Information technologies are designed to make information sharing easy, which is potentially antithetical to the security risk management mission. Furthermore, network users crave convenience and, therefore, are motivated to circumvent security risk management methods, also known as security controls in the security vernacular.

People plus information technology is a recipe for information compromise. Software and hardware configured to work in harmony and perform at scale will inevitably suffer from flaws that are exploited by individuals with varying agendas and a lot of time on their hands. In addition, network users frequently behave in ways that make the attacker's job easier. Exploiting such behavior is the basis for certain attacks, most notably social engineering.

The specter of relentless attacks, no shortage of attackers, and the prominent role of technology in information management compel cybersecurity professionals to concentrate on addressing vulnerabilities via technical solutions. Although an exclusive focus on such vulnerabilities might be operationally expedient, a comprehensive strategy must include a more expansive view of cybersecurity risk.

Unfortunately, cybersecurity professionals often face a difficult choice due to time and resource constraints. Tactical issues become priorities because the clock begins ticking immediately after vulnerabilities are published. In addition, a restrictive cybersecurity strategy can place security professionals on a collision course with business types who have their own obligations and constraints.

There also appears to be a pedagogical bias in favor of tactical security measures. Many books have been written on specific attacks and vulnerabilities, yet surprisingly little has been published about the actual root causes of cybersecurity incidents. Perhaps tackling these root causes is considered too difficult or not in a Chief Information Security Officer's (CISO) purview. Whatever the reason, the absence of pedagogy with respect to the drivers of cybersecurity risk is conspicuous.

A modern IT environment consists of multiple technologies that support numerous network users. Such environments are routinely if informally described as *complex*,