Center for
21ST Century Security and Intelligence
at BROOKINGS

Strategy, Not Speed
What Today's Digital Defenders Must Learn From Cybersecurity's Early Thinkers

Richard Bejtlich
May 2014

Richard Bejtlich is a nonresident senior fellow with the Center for 21st Century Security and Intelligence at Brookings. He is chief security strategist at FireEye and is a former Air Force intelligence officer.

Change and speed: these two words pervade technology discussions, especially when cybersecurity is involved. Defense and national leaders frequently defend their policies, and suggest new policies, by invoking these terms. The United States Air Force makes the following claim in its *Cyberspace Operations* doctrine document: "Cyberspace's unique attributes and potential for speed require the ability to react to rapidly changing situations."[1] The United States *Department of Defense Strategy for Operating in Cyberspace* cites the "rapid pace of change that characterizes cyberspace" as a reason to "examine new collaborative approaches to cybersecurity."[2] Former National Security Agency and United States Cyber Command leader General Keith Alexander told the House Committee on Armed Services in March 2012 that "in terms of attack, cyber attacks, it is over before you know what happened. These happen at lightning speed."[3] A year later he again emphasized change and speed when speaking to the same committee: "Cyber Command operates in a dynamic and contested environment that literally changes its characteristics each time someone powers on a networked device... The cyber landscape also changes rapidly with the connection of new devices and bandwidth."[4] Michael B. Donley, speaking as Secretary of the Air Force on March 23, 2012, echoed Alexander in a speech on cybersecurity, noting "this OODA loop of observing, orienting, deciding, and acting operates at network speed."[5] The government of the United Kingdom demonstrated a similar concern when it recognized that "in a domain where technology and change are fast-moving, responding effectively will require a consistent and extensive effort."[6]

There is no doubt that aspects of the technology field are indeed dominated by change and speed. Compare the original IBM personal computer released in 1981 with the Apple iPhone 5, first sold in 2012.[7] The iPhone ships with a dual-core 1.3 GHz Apple A6 processor, over 270 times faster than the 4.77 MHz Intel 8088 CPU in the IBM PC. The iPhone has over 1,000,000 times the memory of the PC and over 46,000 times the onboard storage in its cheapest configuration. Whereas the PC could connect intermittently at 300 bits per second to bulletin board systems (BBS) via the telephone and the Hayes Smartmodem (also introduced in 1981), the iPhone is persistently linked to the entire Internet via wireless communication technology at 3G (approximately one million bits per second) or 4G (approximately ten million bits per second) speeds.[8] Given the amazing computational progress made between 1981 and 2014, one would expect the security challenges to have morphed equally beyond recognition.

Commentators cite the explosive growth in the number of malware samples as evidence that the security challenge continues to accelerate and change. For example, the 2013 Kaspersky Security Bulletin noted the company's malware lab processed more than 315,000 malware samples per day in 2013.[9] While the vast majority of the samples affected traditional PCs, the count affecting mobile platforms continued to rise. Of the more than 148,000 mobile malware samples in Kaspersky's library, over 104,000 were discovered in 2013 alone.[10]

Statistics based on processing malware samples suffer from inflation due to double-counting variants of malware families, so looking at security incidents may provide a more accurate estimate of change and speed. The 2013 FireEye Advanced Threat Report offered data on malware active in the wild by counting instances of live compromises detected by the company's technology platform. For example, FireEye identified almost 40,000 "unique cyber security incidents," involving almost 18,000 "unique malware infections due to APT [Advanced Persistent Threat] activity," that generated "over 22 million command-and-control (CnC) communications."[11] Counts of government-identified "intrusions" and "breaches" are even more specific. In March 2013 *The Washington Post* reported that White House official Lisa Monaco, deputy national security adviser for homeland security and counterterrorism, told industry executives that in 2013 federal agents notified more than 3,000 U.S. companies that their computer systems had been hacked.[12]

One approach to mitigating the problem of compromised computers relies upon better engineering and technology. Within the last few years, some private security professionals have called for the creation of a ".secure" ("dot-secure") top level domain (TLD), on parity with the familiar .com, .net, and other TLDs. Among other steps, operators of systems in the .secure domain must implement Domain Name System Security (DNSSEC), Transport Layer Security (TLS) for all Web sessions, and Domain Keys Identified Mail (DKIM) and TLS for Simple Mail

Transport Protocol (SMTP) email.[13] While this private approach is open to any who meet the stated requirements, some in government have called for a "separate, secure computer network to protect civilian government agencies and critical industries like the nation's power grid against attacks mounted over the Internet."[14] Some engineers believe completely replacing the current Internet with a so-called "Future Internet" is the best way forward.[15]

The focus on change and speed, driving the desire to reengineer Internet technology, prompted action by the National Science and Technology Council within the Executive Office of the President. In December 2011 they released a report titled *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*. The document introduced the concept of "Trustworthy Cyberspace," claiming that the idea "replaces the piecemeal approaches of the past with a set of coordinated research priorities whose promise is to 'change the game,' resulting in a trustworthy cyberspace... we need enduring cybersecurity principles that will allow us to stay secure despite changes in technologies and in the threat environment."[16] This document and the research effort behind it seek to "change the game" and identify "enduring cybersecurity principles" in order to counter the change and speed of the technology environment. However, it may not be necessary to embark upon another government or private effort to determine how to "secure cyberspace" through technological means. The early days of computer security have much to teach modern practitioners and policymakers. An historical review of security lessons may be a cheaper and more effective way to identify and promote security measures.

Some security analysts have adopted this approach already. In 2013, Jason Healey wrote in his book *A Fierce Domain: Conflict in Cyberspace, 1986-2012* that "cyber conflict has changed only gradually over time; thus, historical lessons derived from past cases are still relevant today (though these are usually ignored)."[17] Whereas Healey's work relied on case studies to support his argument, this paper looks to academic work in the computer security field. A review of noteworthy academic papers from the early years of computer security shows the previous generation of computer security researchers was well aware of the challenges facing their field. Many of the key findings in these documents, ancient by the standards of the technology community, are nevertheless very relevant today. Examining the messages conveyed by these academic papers provides lessons to guide decision maker perceptions of the nature of the cybersecurity challenge. They are one antidote to an unfortunate tendency noted in Healey's book: "all too often these new entrants [to the cybersecurity community] are told to forget everything they thought they knew about security and cyberspace. 'Don't look back — worry about the future... history is in front of you.'"[18] This paper will show that private and public security leaders can make better decisions by understanding discoveries from the 1970s, 1980s, and 1990s.

One of the earliest and possibly most famous studies on computer security was published in 1972. James P. Anderson, on contract with the United States Air Force, led a panel that published a two-volume *Computer Security Technology Planning Study*. As stated in volume one, "the principal unsolved technical problem found by the working group was that of how to provide multilevel resource and information sharing systems secure against the threat from a malicious user."[19] In an age when computers tended not to be networked, the evil insider was the primary threat vector. In a preview of later advice to "build security in," Anderson rejected "security as an afterthought," saying "the reason that an add-on approach, which looks so appealing, will not suffice is that in order to provide defense against a malicious user, one must design the security controls into the operating system of a machine so as to not only control the actions of each user, but of the many parts of the operating system itself when it is acting on a user's behalf."[20] Years later the United States Department of Homeland Security continues to fund the *Build Security In* program to wrestle with the problems of securing software from malicious insiders and outsiders.[21]

Less well known but perhaps more interesting was Anderson's 1980 study *Computer Security Threat Monitoring and Surveillance*. This paper evolved from his 1972 concept of mechanistically stopping malicious insiders, toward detecting their abuse of the system. Anderson sought "to improve the computer security auditing and surveillance capability of the customer's systems."[22] Unfortunately, he discovered that "security audit trails, if taken, are rarely complete and almost never geared to the needs of the security officers whose responsibility it is to protect ADP [automated data processing] assets."[23] Anderson's recommendation involved an anomaly-based approach to intrusion detection, writing "it is possible to characterize the use of a computer system by observing the various parameters available through audit trails, and to establish from the observations, 'normal' ranges for the various values making up the characterizations."[24] He foreshadowed, however, the problems encountered by security analysts in the age of "big data": "when dealing with [IBM's] SMF [System Management Facilities (audit records)], one is overwhelmed with data, a good deal of it not necessarily useful for security audit purposes."[25]

Anderson's work helped launch the intrusion detection field in the academic and later commercial worlds. One of the most significant follow-on papers built on Anderson's work and catalogued reasons to build a so-called "real-time intrusion detection system," i.e., a means to identify intruder activity as it happened. Computer scientists Dorothy E. Denning and Peter G. Neumann wrote *Requirements and Model for IDES - A Real-Time Intrusion-Detection Expert System* in August 1985, and stated the following:

> The development of a real-time intrusion-detection system is motivated by four factors: (1) most existing systems have security flaws that render them susceptible to intrusions, penetrations, and other forms of abuse; finding and fixing all these deficiencies is not feasible for technical and economic reasons; (2) existing systems with known flaws are not easily replaced by systems that are more secure -- mainly because the systems have attractive features that are missing in the more-secure systems, or else they cannot be replaced for economic reasons; (3) developing systems that are absolutely secure is extremely difficult, if not generally impossible; and (4) even the most secure systems are vulnerable to abuses by insiders who misuse their privileges. Thus, a mechanism that could detect intrusions while they are in progress would be extremely valuable, especially if such a mechanism did not have to know about the particular deficiencies of the target system.[26]

Denning and Neumann described conditions familiar to any modern cybersecurity practitioner, well before the invention of the World Wide Web or the widespread adoption of computers in the enterprise. Moreover, they recognized both technical and economic factors affecting computer security. Their solution, IDES, worked to:

> ...examine the audit records as they are generated, update profiles that characterize the behavior of subjects (users) with respect to objects (files, commands, etc.), and ascertain whether current activity is abnormal with respect to the profiles. When an anomaly is detected, it [IDES] will determine whether the security officer should be alerted immediately to a possible intrusion. Periodically, it may also check activity or anomalies accumulated over a time interval.[27]

Crucially, the authors recognized that no technical solution could be fool-proof: They cautioned readers that "a person with enough knowledge about IDES may be able to defeat it through gradual modification of behavior. The goal of IDES is to detect most intrusions and to make it extremely difficult to escape detection."[28] Frustrating the adversary via rapid detection and response, rather than expecting success via prevention, would return several years later in the form of a real-world case study.

In 1986 an astronomer and system administrator at the Lawrence Berkeley National Laboratory (LBNL) pursued intruders within his organization, ultimately revealed as East German agents seeking secrets for the Soviet Union's foreign intelligence service, the KGB. In May 1988, the astronomer, Cliff Stoll, released a paper titled *Stalking the Wily Hacker*, published in the Communications of the Association for Computing Machinery (ACM).[29] Stoll vastly expanded on this paper with his 1989 book *The Cuckoo's Egg*.[30] The analysis in this study is based on the 1988 paper, which helpfully summarizes key points of Stoll's work and findings. Prior to Stoll's paper, no one had documented, in detail, the steps taken to detect and respond to a significant intrusion, let alone one perpetrated over several years by a foreign intelligence service.

Stoll’s first innovation involved casting a wide investigative net because he did not know how the intruders were remotely accessing his systems. Although his initial indicator of compromise was his discovery of a $0.75 accounting error in a Unix system, he needed to catch the intruders live on the network to identify their tools, tactics, and procedures. To this end Stoll instrumented the serial ports providing connectivity to remote users and created a crude alarm system to notify him when suspicious activity appeared to be taking place. In the process, he not only identified the parties responsible for the accounting error but “several other attempted intrusions, unrelated to those of the individual we were following.”[31]

Unlike previous researchers, Stoll concentrated on using a passive, network-based detection system, rather than the host-based, audit-trail-centric approach described earlier. He explained why he preferred the network-centric approach:

> They are invisible even to an intruder with system privileges. Moreover, they gave printouts of the intruder's activities on our local area network (LAN), letting us see his attempts to enter other closely linked computers. A monitor that records keystrokes within an operating system consumes computing resources and may slow down other processes. In addition, such a monitor must use highly privileged software and may introduce new security holes into the system. Besides taking up resources, on-line monitors would have warned the intruder that he was being tracked.[32]

Perhaps most interestingly, Stoll acknowledged the work of other security researchers, saying “we knew of researchers developing expert systems that watch for abnormal activity, but we found our methods simpler, cheaper, and perhaps more reliable.”[33] Using these methods, Stoll observed the intruder trying to access “about 450 computers” using a combination of credentials stolen from previous activity, username and password guessing, and exploitation of unpatched system vulnerabilities.[34] Thanks to his network-based monitoring of the intruder’s command and control channel, he caught activity that was missed on other victim systems.

> Whenever possible, he [the intruder] disabled accounting and audit trails, so there would be no trace of his presence. He planted Trojan horses to passively capture passwords and occasionally created new accounts to guarantee his access into computers. Apparently he thought detection less likely if he did not create new accounts, for he seemed to prefer stealing existing, unused accounts.[35]

Stoll’s campaign to remove or at least restrict the adversary’s freedom of maneuver incorporated many of the standard remediation steps found in modern incident response engagements. Stoll and his team performed host-based remediation, conducted a vulnerability assessment, and continued to monitor. They recognized that there was no such thing as a “secure end state” – only eternal vigilance: “We settled on instituting password expiration, deleting all expired accounts, eliminating shared accounts, continued monitoring of incoming traffic, setting alarms in certain places, and educating our users."[36]

Stoll's experience was clearly an outlier, since he discovered the intrusion himself and pursued it to the point of identifying the intruder as a foreign intelligence agent. In conjunction with Federal and German authorities, Stoll helped prosecute two of the perpetrators. The vast majority of the other victims remained blissfully unaware that they were compromised. By virtue of his instrumentation, Stoll could see the foreign hackers using LBNL computers to try to break into other sites. Stoll wrote: "Of the hundreds of attempted log-ins into computers attached to [the] [I]nternet, only five sites (or 1-2 percent) contacted us when they detected an attempted break-in. Clearly, system managers are not watching for intruders, who might appear as neighbors, trying to sneak into their computers."[37] This problem of not noticing the activity of persistent, stealthy intruders was well-documented by Stoll, and would soon be noticed by a new set of researchers.

In 1988, one of the sister sites to LBNL, Lawrence Livermore National Laboratory (LLNL), acted upon the lessons derived from Stoll's work. Foreign intruders had also targeted LLNL, and the security staff decided to fund three digital security programs in response. They secured funding for anti-virus software, a "Security Profile Inspector" application and a network-based intrusion detection system (network IDS, or NIDS).[38] LLNL approached the University of California, Davis (UC Davis) to create the NIDS, specifically referred to as the Network Security Monitor (NSM). UC Davis professor Karl Levitt enlisted Todd Heberlein, one of his students, to lead the project to create the NSM. In 1990 Heberlein and his colleagues published *A Network Security Monitor*, explaining the tool and tactics that they developed to meet LLNL's needs.

The NSM was the first IDS which directly used network traffic as the data upon which observations were made. Whereas Stoll's instrumentation watched serial lines and sent output to printers, Heberlein's system watched Ethernet local area networks (LANs) and wrote output to computer hard drives. Heberlein built the NSM to keep logs of network activity, regardless of whether any person or algorithm considered them malicious or suspicious at the time of collection. The NSM also generated alerts when it observed suspicious actions worthy of an administrator's attention: "Probabilistic, rule-based, and mixed approaches are being employed by the monitor, and it raises alarms for the Security Officer upon detecting anomalous behavior. The Security Officer interfaces with the monitor via a user-friendly window system, using which he/she can manually alter (usually refine) the monitor's focus as well."[39]

Heberlein's paper described attack patterns and how those steps towards compromising a victim system would appear in the NSM's logs. His two simple patterns reflected the dominant tactics seen in the modern world, so-called "server-side" and "client-side" attacks. He wrote: "For A [Attacker] and T [Target] to communicate, T must either offer a service which can be exploited by A [a server-side attack], or T must seek to use a service offered by A [a client-side attack]."[40] To identify that something malicious was happening, the NSM levied several analytical techniques, embodied in rules: "These rules look for traffic patterns the author, the writer of the rules, imagines an attack will generate. The prototype is currently looking for very simple patterns: a single host communicating with more than fifteen other hosts, logins (or attempted logins) from one host to fifteen or more other hosts, and any attempt to communicate with a non-existent host."[41] Rules such as these would become more popular in the later part of the 1990s, with the arrival of commercial NIDS technology.

Finally, Heberlein's paper asked the "now what?" question familiar to those who receive alerts from any sort of intrusion detection system: "The biggest concern was the detection of unusual activity which was not obviously an attack. Often we did not have someone to monitor the actual connection, and we often did not have any supporting evidence to prove or disprove that an attack had occurred."[42] Heberlein's proposed solution, which eventually became a core feature of the NSM, foreshadowed the modern network forensics platform: "One possible solution would be to save the actual data crossing the connection, so that an exact recording of what had happened would exist."[43] This is the approach adopted by commercial network forensics platforms first released in the 2000s.

The fifth and final example of an academic paper with lessons for modern readers is *The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment*, published by David R. Safford, Douglas Lee Schales, and David K. Hess from the Texas A&M University (TAMU). The authors described how intruders (called "crackers" in the paper, to differentiate them from "hackers," who may be friendly or malicious) compromised some of the 12,000 TAMU Unix computers in August 1992.[44] The paper built upon the issues introduced by Stoll several years earlier by highlighting the dilemmas of immediately removing an intruder from the environment versus watching and learning from adversary activity.

When administrators or security personnel first identify malicious users on computers, they have a natural tendency to want to quickly cut off access and "sterilize" the "infection." Typically, the initial discovery of unauthorized activity is a "tip of the iceberg" event, as demonstrated by Stoll's intrusion. If the security staff acts too quickly, they might remove the only means by which they can understand the intruder's reach and the incident's scope.

The TAMU researchers documented their thought process concerning the dilemma: "It was decided to monitor network connections to the workstation, and, if necessary, disconnect the machine from the net electronically. This decision to monitor the machine's sessions rather than immediately securing it turned out to be very fortunate, as the monitoring provided a wealth of information about the intruders and their methods."[45] By watching the intruders in a deliberate manner, the TAMU team reversed their initial assessment that their opponents were unskilled operators.

> [I]t appeared that there were actually two levels of crackers. The high level were the more sophisticated with a thorough knowledge of the technology; the low level were the 'foot soldiers' who merely used the supplied cracking programs with little understanding of how they worked. Our initial response had been based on watching the latter, less capable crackers and was insufficient to handle the more sophisticated ones.[46]

Once TAMU used network monitoring to better understand the scope of the intrusion and the nature of their foes, they turned to the question of remediation. How should they proceed to remove intruders from the campus?

> After much deliberation, it was decided that the only way to protect the computers on campus was to block certain key incoming network protocols, re-enabling them to local machines on a case by case basis, as each machine had been cleaned up and secured. The rationale was that if the crackers had access to even one unsecure local machine, it could be used as a base for further attacks, so it had to be assumed that all machines had been compromised, unless proven otherwise.[47]

Their assumption that all systems were compromised, and that remediation must be based on that assessment, is a strong warning to security and business leaders of the modern age.

The TAMU incident, similar to the Stoll incident in its willingness to share operational details, offers one more lesson: security must take into account user privacy concerns. TAMU was sensitive to the prospect of capturing user data as the security team tracked intruders on campus networks.

> [M]any may question the ethics and legality of such monitoring. We feel that our current system is not a privacy intrusion. The TCPLOGGER and UDPLOGGER [TAMU monitoring software] are simply the network equivalent of process accounting, as they log routine network events, but none of the associated user level data associated with the event. Etherscan [another TAMU monitoring tool] similarly reports unusual network events, which is the network equivalent of logging failed login attempts.[48]

The question of how to collect and analyze network and other computer data remains important in the current era of computer intrusions.

Summarizing the lessons from these five sets of pioneering computer security authors provides a wealth of guidance for modern security professionals. In 1972 and 1980 Anderson stressed the need to “build security in,” to use audit trails to identify suspicious behavior and to beware the avalanche of “big data” that could overwhelm security analysts. In 1985 Denning and Neumann advocated the need for real-time intrusion detection because all systems have flaws, systems are difficult to replace, developing new "secure" systems is "generally impossible" and even the most secure systems are vulnerable to insiders. In 1988, Stoll practiced and preached the instrumentation of networks in order to scope the extent of an intrusion but to do so in a way that prevents the adversary from detecting the defender’s actions. Stoll also learned and documented that self-discovery of intrusions is exceptionally rare and that eternal vigilance following a breach is the best way to reestablish trust in computing infrastructure.

In 1990, Heberlein implemented a system to record network activity regardless of whether it's known to be good or bad at the time of observation. He also warned security staffs of server-side and client-side attack patterns, and suggested a network forensics approach to answer the "now what" question following a breach. Finally, in 1983 the TAMU team cautioned against cutting off intruders too quickly. They replaced theories of adversary activity with truth derived from monitoring the adversary. Based on their observations, they assumed all systems were compromised, validated the effectiveness of remediation via monitoring and worked to preserve privacy despite difficult security conditions.

With lessons summarized, the question remains: why is no one listening? One possibility is that the research was done under auspices that would not have garnered the attention of serious government or business leaders. Assuming that government-sponsored research is considered worthy of review, the nature of the papers would reject this argument. Of the five author teams covered, only the TAMU group conducted its research and work under private conditions. Anderson wrote his papers for the United States Air Force. Denning and Neumann wrote for the Space and Naval Warfare Command (SPAWAR) and the National Science Foundation (NSF). Although Stoll wrote his paper for the Communications of the ACM magazine, he noted his manuscript was supported by the United States Department of Energy. Lastly, Heberlein’s work answered requirements set by LLNL and was eventually used by the United States Air Force, bringing that service’s role full circle.

A second possibility involves the fact that the papers cited here were but a group of many released by academics during the early years of computer security research. Critics could see them as one set of opinions intermingled with other sets of opinions. The papers in question, for example, do not attempt to create scientific trials or disprove any null hypotheses. Their results are not likely to be replicated at other locations. It is difficult to simulate the activity of a state-sponsored espionage ring operating within military and academic networks.

Furthermore, the software available to instrument networks was less available and more primitive than modern offerings. The open source movement did not begin to accelerate until the mainstream arrival of Linux platforms in the mid and late 1990s. This hypothesis is tougher to disprove.

A third possibility is that these papers tended to promote a monitoring-centric philosophy rather than a prevention-oriented approach. Papers by Stoll, Heberlein, and TAMU were informed by their authors' direct contact with intruders. This experience taught the researchers that security is a challenging operational problem and that knowledge of real-world activity is a requirement for sound policy. Anderson, Denning, and Neumann appear to have leveraged rational thinking about security issues to reach similar conclusions. If watching for disasters is the only realistic answer, the security community can appear despairingly fatalistic. Technology or tactics promoting prevention have an inherently more hopeful message. This hypothesis bears further scrutiny.

The idea that intrusion detection was a hopeless approach gained serious attention in 2003. In June of that year, security market research firm Gartner, Inc. issued a press release with the following title: "Gartner Information Security Hype Cycle Declares Intrusion Detection Systems a Market Failure; Money Slated for Intrusion Detection Should Be Invested in Firewalls."[49] Gartner wrote "IDSs have failed to provide value relative to its costs and will be obsolete by 2005... IDS technology does not add an additional layer of security as promised by vendors... Gartner recommends that enterprises redirect the money they would have spent on IDS toward defense applications such as those offered by thought-leading firewall vendors."[50] IDS users at the time asked themselves "if you can detect it, why can't you prevent it?" In the desire to gain ever more accurate and rapid identification of security incidents, detection-oriented vendors found themselves in a conceptual corner. The rise of so-called "intrusion prevention systems," or IPS, promised to stop security incidents. One vendor, Internet Security Systems (ISS), trumpeted its Proventia product as security's "silver bullet."[51]

Some years later, numerous press and analyst reports have reversed the negative connotations associated with a detection-oriented approach to digital security. Security consulting and software firm Mandiant had advocated detection and response as necessary countermeasures since the company's founding in 2004. In 2010, for example, the firm's first "M-Trends" report, titled *M-Trends: The Advanced Persistent Threat*, advocated "robust logging" and other detection-oriented approaches.[52] The author's own recommendations, documented at his blog since 2003 and in books since 2004, advocated similar countermeasures.[53] By January of 2014, online magazine *Network World* had summarized the sentiment across the industry by writing "Is rapid detection the new prevention?" with a subtitle “Knowing it's impossible to stop every attack, some companies are shifting their security mindset to quickly detect and respond to threats.”[54]

Despite these swings in sentiment away from and then toward monitoring-centric approaches, public and private leaders appeared wedded to the notion that change and speed were the dominant features of the cyber environment. “Changing the game” seemed to be more important than simply watching intruders break into systems. The iPhones of the 2010s were much more powerful than the PCs of the 1980s, and so many more malware samples and incidents were happening. Despite those technological truths, one factor in security incidents remained fairly unchanged.

Human operators are the one constant that tie the PC of the 1980s to today’s smartphones, tablets, laptops, and other platforms. A person could use a computing device from either age for good or for evil. In the modern age, criminals, spies, and other actors manipulate computers and their data for personal and national gain. Humans do not act at “network speed” or “lightning speed.” Jason Healey noted this phenomenon in his 2013 book when he wrote “the most meaningful cyber conflicts rarely occur at the ‘speed of light’ or ‘network speed.’ While tactical engagements can happen as quickly as our adversaries can click the Enter key, conflicts are typically campaigns that encompass weeks, months, or years of hostile contact between adversaries, just as in traditional warfare.”[55] While it is true that technology is always changing, tools are only one element of many when considering digital security. A truly strategic approach integrates many more levels of understanding in order to guide decision makers.[56]

Joint Publication 1 (JP-1), Doctrine for the Armed Forces of the United States, helps illuminate the strategic approach to digital security. JP-1 defines three levels of warfare: strategic, operational, and tactical.[57] Above the strategic level one can place the overall goal of the digital security program, as one might place the overall goal of a military or political endeavor. Below the tactical level one can similarly place tools or technology, the weapons one might employ when conducting tactical maneuvers. Taken as a whole, the five levels appear as shown in Figure 1.

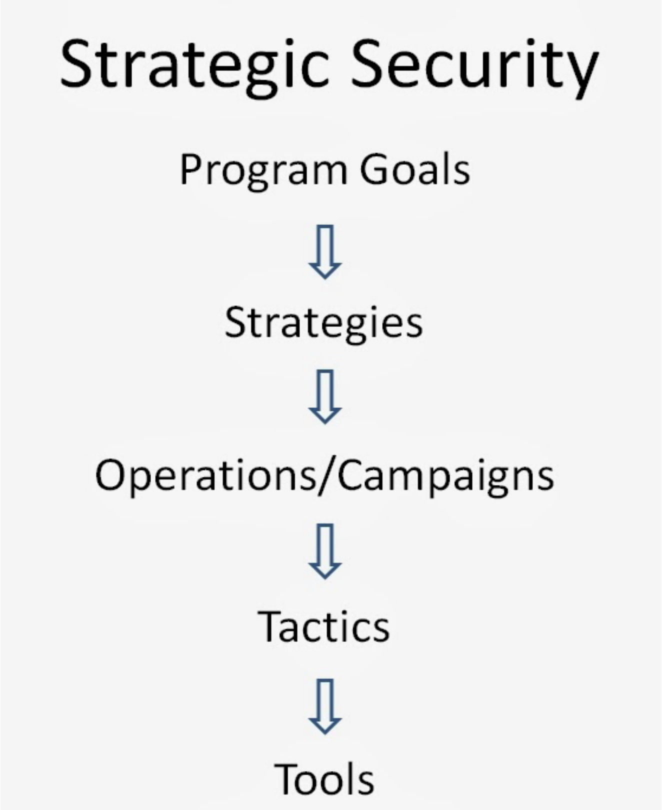
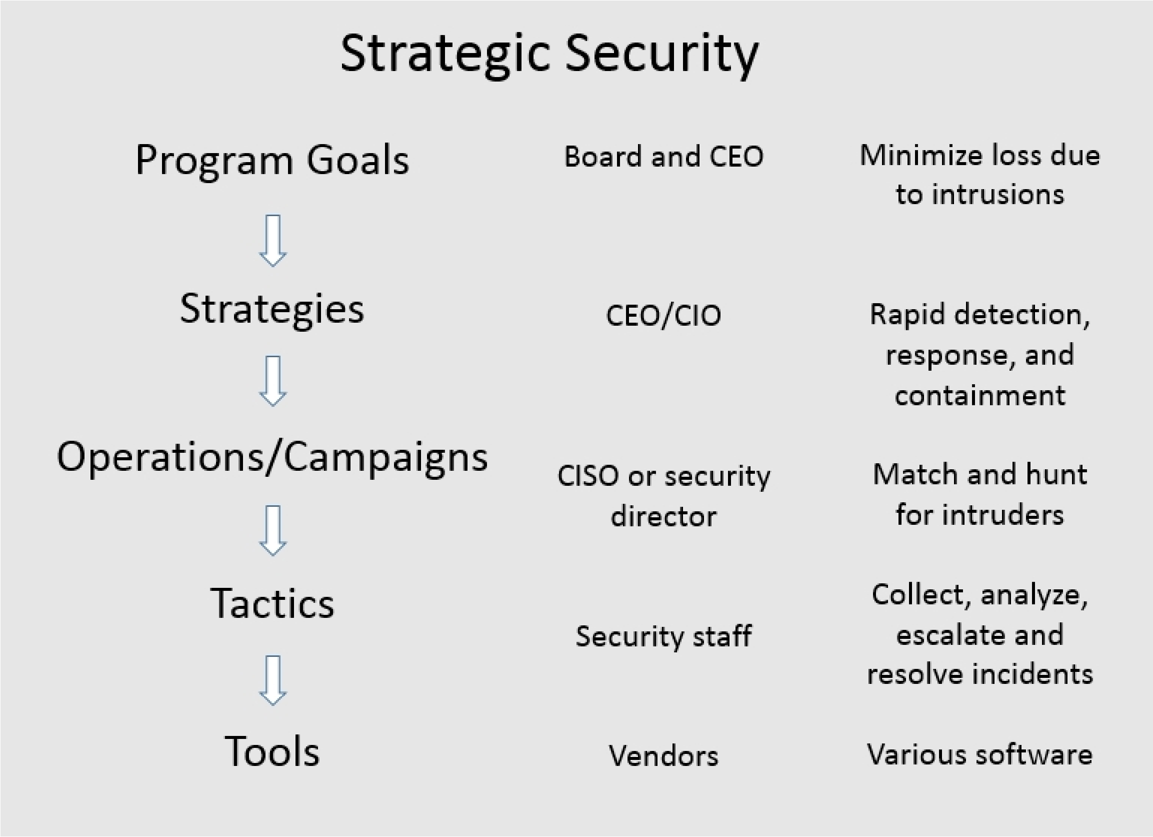


Figure 1. Five Levels of Strategic Security

Using a strategic security framework, a digital defender can build a more effective and durable program. A strategic security system doesn't start with tools and tactics. Instead, it begins by setting one or more overall mission goals. The strategy-minded chief information security officer (CISO) obtains executive buy-in to those goals, which works at a level understood by technicians and non-technicians alike. Next the CISO develops strategies to implement those goals, organizes and runs campaigns and operations to support the strategies, helps his team use tactics to realize the campaigns and operations, and procures tools and technology to equip his team.

Figure 2 shows an example of one strategic security approach to minimize loss due to intrusions, using a strategy of rapid detection, response, and containment, and NSM-inspired operations/campaigns, tactics and tools.



Strategic Security

Program Goals	Board and CEO	Minimize loss due to intrusions
⇩		
Strategies	CEO/CIO	Rapid detection, response, and containment
⇩		
Operations/Campaigns	CISO or security director	Match and hunt for intruders
⇩		
Tactics	Security staff	Collect, analyze, escalate and resolve incidents
⇩		
Tools	Vendors	Various software

Figure 2. Five Levels of Strategic Security Example

Most security professionals, and by association policymakers and leaders taking advice from those practitioners and engineers, fixate on the tools, and to a lesser degree, the tactics of the digital security problem. Goals, strategies, and campaigns aren't usually a consideration because technicians, administrators, programmers, and the like spend their time working with tools. To the extent that they think about creative ways to use those tools, that would account for tactics. The communities which tend to think in terms of goals, strategies, and campaigns – think tanks, policy analysts, and so on – have traditionally not engaged with the technicians to bring the entire strategic security approach to bear on modern challenges.

The strategic approach's attraction in digital security is that practitioners can place lessons like those derived from academic papers within the framework, and decide if they remain relevant. The lessons described earlier primarily center on strategies, operations/campaigns, and partially on tactics. None of them describe specific tools, although many of them require tools in order to be put into practice. As shown in Figure 2, detecting intruders is actually shorthand for a rich strategic security program, one whose goal is minimizing loss through a strategy of rapid incident detection, response, and containment. Security teams run operations to match threat intelligence against security event data and hunt for novel intruders as needed. They tactically collect, analyze, escalate, and resolve incidents and the related data using tools suited for those functions.

It is crucial, however, that the ultimate goal and strategy remained linked with the tools at the bottom of the process. If that chain decouples, the outcome could be disastrous, where technical reality makes strategic theory obsolete. For example, a program built on monitoring the network will fail if all network traffic is encrypted. The tools at the bottom of the process will not be able to "see" the contents of network traffic and will be less effective when trying to identify suspicious and malicious activity. In this dysfunctional case, the program goal will not be achieved because the tools cannot deliver the required data to the personnel conducting tactical endeavors and operational campaigns.

This paper proposed that the early computer security literature offers rich lessons for digital defenders of all ages. Although the technology used by friends and foes alike continues to evolve at a blistering pace, the manner in which defensive tools can be leveraged has not dramatically changed. Electrons may move at "network speed," but adversaries continue to conduct significant malicious activity at human speed. A focus on monitoring to enable rapid detection and response, identified in the 1970s, 1980s, and 1990s continues to be relevant in the 2010s and will likely continue into the next decade. Digital defenders would benefit from learning about and adopting a strategic security program that tightly links tactics and tools with program goals, strategy and campaigns.

[1] United States Air Force, *Air Force Doctrine Document 3-12, Cyberspace Operations, 15 July 2010, Incorporating Change 1, 30 November 2011* (Maxwell Air Force Base, Alabama: Curtis E. LeMay Center for Doctrine Development and Education, 2011), 29.

[2] United States Department of Defense, *Department of Defense Strategy for Operating in Cyberspace, July 2011* (Washington: United States Department of Defense, 2011), 8.

[3] House Committee on Armed Services, *Budget Request for Information Technology and Cyber Operations Programs: Hearing Before the Subcommittee on Intelligence, Emerging Threats, and Capabilities, Committee on Armed Services, House of Representatives*, 112th Cong. (March 20, 2012) (statement of General Keith B. Alexander, Commander, United States Cyber Command).

[4] House Committee on Armed Services , *Information Technology and Cyber Operations: Modernization and Policy Issues to Support the Future Force: Hearing Before the Subcommittee on Intelligence, Emerging Threats, and Capabilities, Committee on Armed Services, House of Representatives*, 113th Cong. (March 13, 2013) (statement of General Keith B. Alexander, Commander, United States Cyber Command).

[5] Michael B. Donley, "Remarks," Lecture, CyberFutures Conference, National Harbor, MD, March 23, 2012. http://www.thefreelibrary.com/CyberFutures+conference+remarks.-a0288627492.

[6] Office of Cyber Security and Information Assurance in the Cabinet Office, *Cyber Security Strategy: Protecting and Promoting the United Kingdom in a Digital World* (London: Cabinet Office, November 25, 2011), 5.

[7] John Breeden II, "30-Year Showdown: IBM PC vs. Apple iPhone," *Government Computing News,* May 29, 2013. http://gcn.com/Articles/2013/05/30/Comparisons-IBM-PC-iPhone5.aspx.

[8] Brian Nadel, "3G vs. 4G: Real-world Speed Tests," *ComputerWorld*, December 15, 2010. http://www.computerworld.com/s/article/9201098/3G_vs._4G_Real_world_speed_tests.

[9] Kaspersky Lab Global Research and Analysis Team, *Kaspersky Security Bulletin 2013*, (Moscow: Kaspersky Lab, December 10, 2013), 35. http://media.kaspersky.com/pdf/KSB_2013_EN.pdf.

[10] Ibid.

[11] FireEye Labs, *FireEye Advanced Threat Report: 2013*, (Milpitas, CA: FireEye Labs, February 2014), 2. http://www.fireeye.com/blog/technical/malware-research/2014/02/the-2013-fireeye-advanced-threat-report.html.

[12] Ellen Nakashima, "U.S. Notified 3,000 Companies in 2013 about Cyberattacks," *Washington Post*, March 24, 2014. http://www.washingtonpost.com/world/national-security/us-notified-3000-companies-in-2013-about-cyberattacks/2014/03/24/74aff686-aed9-11e3-96dc-d6ea14c099f9_print.html.

[13] Kelly Jackson Higgins, "New .secure Internet Domain on Tap," *Dark Reading*, May 10, 2012. http://www.darkreading.com/new-secure-internet-domain-on-tap/d/d-id/1137674?.

[14] Tom Shanker, "Cyberwar Chief Calls for Secure Computer Network," *New York Times*, September 23, 2010. http://www.nytimes.com/2010/09/24/us/24cyber.html?_r=0.

[15] One example is the Future Internet Architecture Project, http://www.nets-fia.net/.

[16] Executive Office of the President, National Science and Technology Council, *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*, (Washington, DC: Executive Office of the President, December 2011), vii, ix.

[17] Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (Vienna, VA: Cyber Conflict Studies Association, 2013), 10.

[18] Ibid.

[19] James P. Anderson, *Computer Security Technology Planning Study, ESD-TR-73-51, Volume 1*, (Hanscom AFB, Bedford, MA: Deputy for Command and Management Systems, Headquarters Electronics Systems Division, October 1972), iv.

[20] Ibid.

[21] Build Security In Website, https://buildsecurityin.us-cert.gov/.

[22] James P. Anderson, *Computer Security Threat Monitoring and Surveillance*, (Fort Washington, PA: James P. Anderson Co., April 15, 1980), 1.

[23] Ibid., 2.

[24] Ibid., 19.

[25] Ibid., 40

[26] Dorothy E. Denning, and P.G. Neumann, *Requirement and Model for IDES - A Real-Time Intrusion Detection System, Technical Report # 83F83-01-00,* (Menlo Park: Computer Science Laboratory, SRI International, 1985).

[27] Ibid.

[28] Ibid.

[29] Cliff Stoll, "Stalking the Wily Hacker," *Communications of the ACM* 31, no. 5 (May 1988): 484.

[30] Cliff Stoll, *The Cuckoo's Egg* (New York: Pocket Books, 2005).

[31] Stoll, "Stalking," 485-486.

[32] Ibid., 486.

[33] Ibid.

[34] Ibid., 489.

[35] Ibid., 490.

[36] Ibid., 491.

[37] Ibid., 495.

[38] Richard Bejtlich, *The Practice of Network Security Monitoring*, (San Francisco: No Starch Press, 2013), xx.

[39] Todd L. Heberlein, et al, "A Network Security Monitor," in *Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy*, edited by Deborah Cooper and Teresa Lunt (Washington, DC: IEEE Computer Society, 1990), 296.
[40] Ibid., 298.
[41] Ibid., 300.
[42] Ibid., 302.
[43] Ibid.
[44] David R. Safford, et al, "The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment," updated version of a paper that first appeared in *Proceedings of the Fourth USENIX Security Symposium* (Berkeley, CA: USENIX Association, 1993).
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Ibid.
[49] Gartner, Inc. "Gartner Information Security Hype Cycle Declares Intrusion Detection Systems a Market Failure; Money Slated for Intrusion Detection Should Be Invested in Firewalls," *Businesswire*, June 11, 2003, http://www.businesswire.com/news/home/20030611005056/en/Gartner-Information-Security-Hype-Cycle-Declares-Intrusion.
[50] Ibid.
[51] Richard Bejtlich, "Deflect Silver Bullets," *TaoSecurity Blog*, November 5, 2007, http://taosecurity.blogspot.com/2007/11/deflect-silver-bullets.html.
[52] Mandiant, *M-Trends: The Advanced Persistent Threat*, (Alexandria, VA: Mandiant Corp., 2010).
[53] See http://www.taosecurity.com/books.html for a comprehensive listing.
[54] Bob Violino, "Is Rapid Detection the New Prevention," *Network World*, January 2, 2014. http://www.networkworld.com/news/2014/010214-outlook-security-277111.html?hpg1=bn.
[55] Healey, *A Fierce Domain*, 15.
[56] In the author's experience, the majority of digital security staffs and leaders concentrate on the tools and tactics of the trade, and do not consider other aspects of strategic thought. This phenomenon is similar to thinking in the Air Force prior to the publication of Colonel John Warden's book *The Air Campaign* and its subsequent influence on the air campaign in the first Gulf War.
[57] United States Department of Defense, *Joint Publication 1, Doctrine for the Armed Forces of the United States, 25 March 2013* (Washington, DC: United States Department of Defense, 2013), I-7 - I-8. http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

Center for
21ST Century Security and Intelligence
at BROOKINGS

The Center for 21st Century Security and Intelligence (21CSI) in Foreign Policy at Brookings was created to address the key issues shaping security policy over the coming decades. The Center seeks to answer the critical questions emerging in defense, cybersecurity, arms control, and intelligence in an all-encompassing manner, seeking not just to explore important new policy challenges but also how they cross traditional fields and domains. Under the leadership of Peter W. Singer, one of the world's leading experts on changes in warfare, the Center focuses on delivering cutting-edge research, analysis and outreach that shapes public understanding and official decision-making across a broad range of security issues.

The views expressed in this piece are those of the author and should not be attributed to the staff, officers or trustees of the Brookings Institution.