FATHOM5
SECURING THE DIGITAL FUTURE

WHITE PAPER

THE SECOND AGE OF CYBER

Philosophy and Principles to Shift the Advantage to the Cyber Defender

Executive Summary

The First Age of Cyber has been characterized by the exploitation of digital assets through small subsystem vulnerabilities, which has provided a clear advantage to cyber attackers for the last 30 years. The opportunity to apply a new philosophical approach to shift the balance of power toward a defenders' advantage is made possible by technologies and processes that have emerged over the last five years.

The Second Age of Cyber requires moving away from the philosophy that has governed cybersecurity since the appearance of the first computer virus. The Second Age begins by rejecting the notion that networks have a physical metaphor and is enabled by knowledge-based networks, not hierarchies.

These two philosophical shifts lead to specific, measurable principles for the Second Age of Cyber that when implemented create advanced cyber defenses that can prevent catastrophic system or data loss, automatically handle known pathogens, and adapt at machine speed to new threats.

Fight Adversaries, Not checklists

Adversary-focus takes the emphasis off of certification and mandates thinking beyond traditional metrics to understand whether defenders are winning or losing an engagement against a field of potential adversaries.

Use Machines to Combat Machines

Prioritize architectures and processes that pool data and provide a platform for algorithms. By deploying algorithms, the concept of infrastructure can be transformed from devices that need to be monitored and optimized into sensors that increase understanding of the adversary.

What You Don't Know, Will Hurt You

Understanding whether there is abnormal activity in a system is more important than the knowledge of a vulnerability. The former tells you what resources are at risk and allows real-time operational risk assessment, whereas the latter cannot be correlated to operational risk.

Shape the Battlefield

Shaping and reshaping cyber terrain is a low-cost way to outpace an attacker's ability to map the network and develop plans for information exploitation.

You are What you Measure

The use of holistic metrics such as cycle time for an emerging risk to become remediated automatically, prioritized by severity and risk, allows Second Age principles to be incorporated into organizational surveillance and response.

Organizations that adopt the Second Age philosophy and implement the principles can shift the balance of power in cyberspace in favor of defenders and reap the benefits of:

- **Real-time adversary focused metrics**
- **Prioritized application of remediation tools and software**
- **Quantifiable return on cybersecurity capital investment**
- **Measurable decreases in the risk of catastrophic data loss or system incapacitation**

The First Age of Cyber

The Maginot Line was built by the French in the 1930's as a defense against German invasion. The French assimilated their past experience in WWI and at a cost of 3 billion francs ($1.5 Trillion in USD today) to create a structure impervious to the forms of attack they believed were coming. The French were thorough and meticulous in their expensive design, protecting against aerial assault and shelling from tanks. They took great care to scan the latest in technological innovations and incorporated defense-in-depth, as depicted in Figure 1. However, despite technological innovation, defense-in-depth, and billions of francs, the German maneuver force attacked via the least defended route through Belgium and successfully invaded France on the 10th of May 1940. They entered Paris one month later proving the Maginot Line useless.

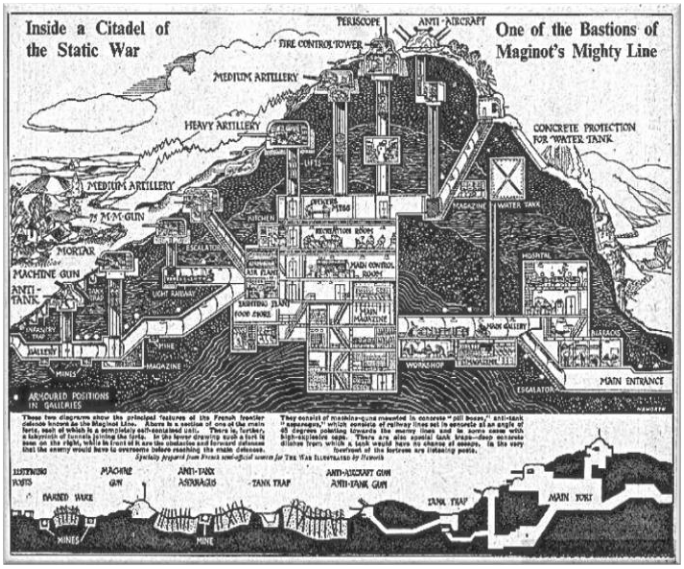

Figure 1. The Maginot Line included defense-in-depth and meticulous inspection and certification of components.

Image Credit: https://i1.wp.com/militaryhistorynow.com/wp-content/uploads/2017/05/topfotomaginotcrosssection-1.jpg

Similarly, in 1988 Robert Tappan Morris saw a way to get around the nascent computer security protections of the early Internet by exploiting vulnerabilities he found in Unix Sendmail and remote shell execution. The program Morris wrote would come to be known as the *Morris Worm* and is widely considered the first computer virus. Since then almost every instance of computer security failure has followed the pattern of attackers finding one or two vulnerabilities in a complex suite of software and then creating exploits that amplify those vulnerabilities to circumvent defense-in-depth. Just like the Germans invented Blitzkrieg to exploit the poorly defended Belgian border for their access route into France, information security professionals have been as ineffective in defending national and enterprise digital resources as the Maginot Line was in defending France.

In the aftermath of the Morris Worm, DARPA directed the founding of the first Computer Emergency Response Team (CERT). Early CERTs used physical world protection and response constructs, like fire departments, as their paradigm for network security.[1] This metaphor led to conceptual errors in thinking. Treating networks like physical assets that can be protected and focusing organizational assets on response creates an untenable model for security. The notion of a barrier around a network is a fallacy, because exploits are delivered or controlled through small unknown or unfixable subsystem vulnerabilities. This is in addition to the fact cyber defense is hampered by hierarchical organizational constructs with linear up/down information flows.

As long as we believe that cyber defense consists of chasing after ever-shifting subsystem vulnerabilities we remain in the First Age of Cyber and attackers have the advantage.

[1] Killcrece, Kossakowski, Ruefle, and Zajicek. 2003. "State of Practice of Computer Security Incident Response Teams (CSIRTs)." Carnegie Mellon Software Engineering Institute. p. 11.

The Second Age of Cyber

Cyberwar is now a defining feature of modern conflict with strategic and existential business consequences and, tragically, defenders seldom win. The list of government resources stolen by cyber espionage includes everything from plans for the United States most advanced fighter jet to the personally identifiable information of every American with security clearance.[2] Beyond information systems, the cyber-physical world that includes utilities, infrastructure and military equipment has created a new class of Internet connected risks, where physical assets are susceptible to cyberattack, as demonstrated by the impact of the Stuxnet virus on the Iranian nuclear facilities and the 2015 takedown of the Ukrainian power grid by Crash Override malware.

Cyber risks have grown to strategic importance as critical information systems, the shipping and transport industry that create global trade, and military hardware have become more connected. Yet, there is hope, because as these risks have matured so have the techniques available to information defenders. Recently, the tools, techniques, and organizational constructs have come into existence to shift the offense-defense balance from attackers to defenders. However, this shift is far from inevitable and requires a Second Age of Cyber marked by a fundamental shift in philosophy and in the intelligent design of a new class of defensive organizations and systems.

The Second Age of Cyber dawns when the offense-defense balance shifts away from cyber-attackers to cyber-defenders as a result of organizational transformation, knowledge-based networks, and defined, reliable, and repeatable metrics of success.

Philosophy of the Second Age of Cyber

The Second Age of Cyber requires two fundamental shifts away from the philosophy that has governed cybersecurity for the last 30 years. First, rejecting the notion that networks have a physical metaphor lays the foundation for new approaches to the problem; and second, understanding that cybersecurity requires knowledge-driven networks, not hierarchies creates the organizational structure for these approaches to succeed.

Networks are not Physical

The first philosophical shift is understanding that effective techniques in physical security do not translate to the cyber domain. Currently the cybersecurity marketplace is dominated by vendors capitalizing on the physical security construct by creating analogies and products that mimic the physical world (i.e. access controls and perimeter defenses). However, these tools have led to a false sense of security that belies the truth: networks are porous by design and no infrastructure-based solution has proved to be effective at protecting networks of global enterprise organizations.[3]

The porous nature of networks is driven by the reality that the transmittal of new data and new types of data is what makes a network useful to users in the first place. A network's value is correlated to its ability to pass data and ever-changing data types and formats ingested by a continually evolving application suites. A network is only as valuable as the information that moves through it. Therefore, the tension between network function and network security is a forced dilemma created by the idea that security is infrastructure-dependent and can be enforced at the perimeter.

---

[2] https://www.theguardian.com/australia-news/2017/oct/12/secret-files-on-jets-and-navy-ships-stolen-in-extensive-and-extreme-hack

https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

[3] Data losses from Equifax, Anthem Healthcare, Target, Sony, Home Depot highlight the susceptibility of global organizations.

In reality, a network has no "perimeter" to secure because of undocumented inter-network connections between sub-networks, exponential growth in connected devices, adoption of the cloud, and implementation of Software-as-a-Service into core organizational functions. We cannot "lock every door" because there are an infinite number of doors and each one creates known and unknown vulnerabilities in the millions of software tools running on the network. No one can build the digital Maginot Line to keep out malicious actors because, by design, networks must let through all of an organization's legitimate traffic and by extension malicious actors will find a way to conform to the gigabyte highway of traffic that is crossing the wall every second.

By rejecting the notion that a network is physical, defenders can move away from fixating on device configuration and instead become adversary-focused and data-centric. This concentrates their energy on the sensors, data, and algorithms that provide insight into what is happening in real-time within their network instead of logging what happens at the perimeter and the endpoints. They are less concerned with having the right box that meets static certification criteria and more focused on understanding adversaries that are touching and moving in and around their network. The best organizations in the Second Age will have metrics to measure whether they are winning or losing an engagement with an adversary that is calculated in real-time and derived from data gathered using the broadest possible surveillance.

A similar transition was required by the public health community with regards to infectious disease. In the early 1900s the focus of infection control efforts was on sanitation and inoculation, which mirror the current certification and software patching approach to network operations. By mid-century it was clear that while having sanitation systems and vaccines was a necessary first step, it did nothing to combat emerging threats. Analogous to emerging infectious disease, ***malware is continually and rapidly evolving, and the greatest risk exists before an emerging infection has been detected. Practitioners must shift their focus away from physical solutions to developing new organizational constructs and metrics,*** which is what took infectious disease from the leading cause of global death to a manageable risk.

KNOWLEDGE-DRIVEN NETWORKS, NOT HIERARCHIES

Identifying emerging pathogens, whether human or cyber, requires prioritizing wide-area surveillance, data-sharing, and real-time classification of emerging risks. Traditional hierarchical structures are a major barrier to effective cyber defense. First, with emerging threats, both the risk and the knowledge are typically at the edge of the organization. Cyber threats move at network speed, so the edge of the organization must be empowered to respond, and organizational resources should be organized to pivot to where the threat is greatest. ***Time is the critical element in combatting malware, yet by flagging threats and escalating tickets up an organization and then forcing centrally mandated solutions back down, defenders give cyber attackers control of the clock and organizational hierarchy reinforces the attackers advantage.***

Organizational strategy should be centralized, however the decision cycle for combatting emerging threats requires empowering the first responder at the edge. Response is only effective if the time window matches the threat speed. On the bridge of a ship, maneuvering boards are effective, because there is a five-minute time window in which to come to a collective decision. However, in a fighter cockpit, maneuvering boards would be catastrophic, because at supersonic speed there are only seconds to act. In cyber, attacks are arriving at network speed, but currently most organizations have a 5-hour to 5-week decision cycle using ticket escalation systems to push issues up a hierarchy.

In contrast, global health organizations have hierarchical structures responsible for providing resources and directing partners, but the partner organizations are acknowledged to be the experts in their field or geography. The individuals and organizations at the edge are given the autonomy to prioritize and implement guidelines in the way that best serves their population. The central hierarchy is responsible for information sharing, connecting

partners, and providing resources to combat emerging threats. This emphasis on knowledge and prioritization means that a nurse at the front line of an Ebola outbreak may be the most important person in the world of global health at the emergence of an outbreak.

In the Second Age of Cyber the central organization is the conduit through which information is shared between local experts. The central organization creates and cultivates the knowledge-driven network, scales best practices and provides resources to the most effective nodes. Attacks become welcome data points that can be instantaneously shared to improve risk models, surveillance, and response so that the entire system is better defended against serious emerging threats.

Principles of the Second Age of Cyber

These two philosophical shifts lead to specific, measurable principles for the Second Age of Cyber that when implemented create advanced cyber defenses that can prevent catastrophic system or data loss, automatically handle known pathogens, and adapt at machine speed to new threats.

Fight Adversaries, Not Checklists

Organizations spend the majority of their resources fortifying, certifying, and inspecting their networks. For example, in the U.S. Department of Defense security by checklist begins with Security Technical Implementation Guides, flows into Risk Management Framework checklists for obtaining authority to operate, and is routinely enforced in operations by Command Cyber Readiness Inspection checklists. Software vulnerabilities and malware signatures are added to the system and are measured against the checklist of outstanding patches and signatures, rather than against risk metrics.

Checklist driven activities are an artifact of management techniques derived from the industrial age where central leadership produced the criteria to be executed by leaders at lower echelons. This approach is attractive to leadership, because it gives clear criteria against which to align personnel and resources and criteria by which to verify compliance and address discrepancies. However, for the reasons discussed above this approach fails to defend complex global enterprises against cyber attackers. Checklist-focused solutions are sufficient in closed laboratory environments, but examples like Target, Sony, Yahoo, Anthem, Equifax, Maersk, the U.S. Office of Personnel Management and dozens more reveal that high cost, certified, inspected systems are ineffective at preventing exploitation via subsystem vulnerabilities.

Adversary-focus takes the emphasis off of certification and mandates thinking beyond traditional metrics to understand whether defenders are winning or losing an engagement against a particular adversary in real time. Knowing who is attacking and hypothesizing why, gives the cyber defense team context and provides leadership with a clear prioritization strategy for surveillance, alerts and mitigation. Similarly, the public health community does not measure success by how many cases of benign pathogens, like the common cold, they have stopped or the number of vaccinations they have given against eradicated viruses, because these metrics do nothing to prevent morbidity and mortality.

In addition to being ineffective, the infrastructure-focused paradigm leads to ballooning costs without reducing risk. Checklists continue to grow in order to cover emerging threats and new device categories are added creating cost growth. Compliance organizations are rarely responsible for managing financial resources, so costs grow unconstrained without incentive for certifying organizations to consider the financial impacts. By adopting an adversary-focus, it aligns network security to system-wide performance metrics and shifts capital planning toward tools that increase data introspection, thereby allowing cyber leaders to tie their costs to measurable gains in network awareness, risk reduction, and readiness to react to a sighting of the adversary.

Use Machines to Combat Machines

Attackers are developing new methods to use machine learning and artificial intelligence (AI) to automate malware creation and increase the speed and sophistication of attacks.[4] In contrast, most organizations are still focused on component specific security driven by a completely unscalable process – log review. Complicating this further is the inverse relationship between attack complexity and signal-to-noise ratio in the log data. As a result, short-handed teams of analysts are being asked to plow through increasing amounts of information looking for signals that move closer and closer to baseline noise.

Second Age organizations allow machines to do what they excel at and humans to focus on their specialties. Recent advances in machine learning are a key breakthrough for cyber defenders. The one truism of machine learning algorithms is that they generally perform better with increased training data. Organizations must increase data flow and push that flow to machine learning systems. This allows human operators to focus on results and perform cross system synthesis.

The Second Age of Cyber prioritizes architectures and processes that pool data and provide a platform for algorithms. By deploying algorithms, the conception of infrastructure can be transformed from devices that need to be monitored and optimized into sensors that increase understanding of the adversary. Algorithmic-based analysis coupled with adversary-focus provides a contextualized view of attacks. As a result, teams can focus on developing techniques to combat advanced attacks and fixes to the root causes of defensive weaknesses.

What You Don't Know, Will Hurt You

Networks are certified to a set of standards and then given authority to operate. As new threats emerge there is a time lag, typically measured in years, from the sighting of a new cyber-attack technique and the corresponding certification item that addresses it. Therefore, network defenders trained to respond to certification requirements are always lagging attacker capabilities.

Software patches are almost always deployed against known vulnerabilities, but without surveillance resources to indicate if an adversary has already taken advantage of the weakness. Similarly, malware signatures are often tied to a particular threat actor but deployed into network defenses without scanning tools to see if indicators of compromise are already on the network.

Analogously in infectious disease, vaccination against known pathogens is important for prevention, but it is the emerging threat that is most dangerous. Public health organizations empower every health care worker to contribute to surveillance. At the first set of anomalous symptoms the priority becomes identifying, classifying, and pivoting response resources towards a potentially virulent unknown pathogen. In the Second Age, understanding whether there is abnormal activity in the system is far more important than the knowledge of a vulnerability. The former tells you what resources are at risk and allows real-time operational risk assessment, whereas the latter is just knowledge of a theoretical exigency and cannot be correlated to operational risk.

Second Age teams prefer threat intelligence that can be integrated into network surveillance in real-time. Based on those results they prioritize patches and signatures to find, fix, track and target adversaries in their system. Leaders in Second Age Cyber organizations translate adversary knowledge and ongoing operational requirements to prioritize courses of action for engaging adversaries in the network and assessing the outcomes of those plans.

[4] King, Aggarwal, Nikita, Taddeo, and Floridi. 2018. Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. https://ssrn.com/abstract=3183238 or http://dx.doi.org/10.2139/ssrn.3183238

Shape the Battlefield

Most organizations certify their infrastructure and rarely alter the underlying network topology, defensive appliance configuration, or runtime environment, because they are concerned with violating their authority to operate. This static approach to network security all but guarantees a methodical reconnaissance program by cyber adversaries will eventually discover the fixed component in the system with vulnerabilities unknown to the defenders. The compliance regime that compels cyber defenders to remain static misses one of the most important features of the cyber domain – Code is Free!

Shaping and reshaping terrain and defensive fortifications of a physical asset was impossible in the world prior to software. Every new physical fortification requires steel, concrete and manpower acquired by significant additional costs. Conversely, in the cyber domain defensive constructs are simply code that costs virtually nothing to reproduce ad infinitum once the software is written. Specific technologies that implement the principle that configuration is just free code and defeat adversary surveillance (and most assuredly violate static authority to operate) criteria are continuously variable software defined networks (SDNs), randomized container orchestration environments, and randomized runtime environmental variables that create a unique memory layout for each machine. Each of these helps defeat adversary reconnaissance and can be implemented to operate at machine speed that outpaces an attacker's ability to map the network and develop plans for information exploitation.

You are What you Measure

Cybersecurity metrics are divorced from operational awareness and typically fail to measure either the value of investment or how well critical assets are protected. The most commonly used cybersecurity metrics have unintended consequences. Measuring cybersecurity by investment simply incentivizes spending more money. Siloed metrics readily available from vendor products such as counts of incidents, viruses blocked, patches applied, spam blocked, or unsuccessful logons, incentivizes focusing on the known, less malicious threats that are easy to resolve. These data provide a sense of control but do not reduce cybersecurity risk.

In contrast, network reliability uses system-wide real-time network metrics that correlate directly to business function. Public health uses near real-time surveillance metrics, classified by pathogen, with an understanding of the underlying severity and transmissibility, in addition to prevention metrics such as vaccination rates. As long as cybersecurity is treated like IT hygiene, organizations will not have insight into operational risk. The philosophy and principles of the Second Age of Cyber must be reflected in the metrics. Second Age Organizations prioritize surveillance by ***real-time detection of indicators of compromise.*** They are adversary focused and ***tag indicators to adversary campaigns.*** In order to understand operational risk, they ***map where an adversary is in the cyberattack lifecycle***: Reconnaissance, Weaponization & Delivery, Exploitation, Installation, Command-and-Control, Actions on the Objective.[5] This data can then be used to develop metrics that ***classify severity and risk***.

The key to operationally relevant response is how quickly remediation against an emerging threat detected at the edge of the organization or at a partner organization can be deployed against the most critical organizational assets. This requires using machines and automation to reduce cycle time, but metrics related to automated response are a means, not the end state. A holistic metric such as ***cycle time for an emerging risk to become remediated automatically, prioritized by severity and risk,*** allows Second Age principles to be incorporated into organizational surveillance and response. At the enterprise-level, different standards for cycle time can be employed based on severity, risk, and asset priority.

[5] Lockheed Martin Cyber Kill Chain® https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

CONCLUSION

When an organization is built around Second Age philosophy and principles, cybersecurity becomes asymmetric – an attacker must do everything right, but a defender has multiple opportunities to stop a catastrophic loss. The technology and hardware needed to facilitate this transition can be deployed now. Today's advanced network appliances provide rich information about the data flowing through them. The structured representation of threat intelligence data allows the use of machine learning algorithms to execute real-time correlation of network data with adversary actions that can subsequently be linked to operational risk. The automation, software defined networks, and orchestration environments that have emerged over the last five years allow remediation and shaping procedures to maneuver against prioritized threats.

The cumulative result of moving toward the Second Age of Cyber is an operable system for winning engagements in cyberspace. The benefits to organizations include:

- Adversary focused metrics for operational and system risk that update in real-time
- Prioritized application of remediation tools and software based on operational risk
- Quantifiable return on cybersecurity capital investment
- Measurable decreases in the risk of catastrophic data loss or system incapacitation

In contrast, those organizations who focus on optimizing First Age approaches will continue to endure challenges including:

- Compliance based metrics that lag adversary tactics and techniques by years
- Vulnerability patching schemes that are uncorrelated to operational risk
- Capital investment driven by atomic upgrades to "boxes" in the system
- High likelihood of catastrophic data loss and critical operational impacts

Organizations can start by ensuring their network has the components that make it capable of feeding a data-driven environment. Additionally, the culture and structure must change to ensure network engineering teams, security center operators, and users have the development operations (DevOps) processes to move at network speed. The transition to the Second Age starts with educating organizational leadership about the philosophy and principles that will shift the advantage to the cyber defender.

ABOUT FATHOM5

Fathom5 is an industrial cybersecurity company focused on the development of hardware, software, and analytics to visualize and quantify the deep interdependencies in networks in order to detect anomalies in highly complex critical systems. Fathom5 is committed to a Security-First approach focused on the secure deployment of algorithms that embrace the Second Age of Cyber principles. Learn more at https://fathom5.co/

AUTHORS

Zachary Staples and **Maura Sullivan** are the co-founders of Fathom5.

Zachary Staples had a 22-year career in the United States Navy as a surface warfare officer specializing in electronic warfare. His final tour was as the Director of the Center for Cyber Warfare at the Naval Postgraduate School, where he led inter-disciplinary research and development teams exploring cyber capability development. Zac holds a B.S. in engineering from the U.S. Naval Academy, a Masters in National Security Affairs from the Naval Postgraduate School and is a distinguished graduate of the Naval War College.

Maura Sullivan, PhD specializes in systemic risks and data-driven emerging technologies. Maura was the Chief of Strategy and Innovation at the U.S. Department of the Navy, where she developed and implemented the strategic roadmap for emerging cyberphysical technologies. Maura led a start-up business unit within the global catastrophe risk company, RMS, developing software and consulting solutions for managing systemic risks for financial and insurance markets. She was a White House Fellow, has a Ph.D. in epidemiology from Emory University and a B.S and M.S. in earth systems from Stanford University.

Publication date: Rev 3 July 2018