Digital Network Resilience: Surprising Lessons from the Maginot Line

Ray A. Rothrock

ABSTRACT

For most of us today, the phrase "Maginot Line" is a stale but cruel joke, if not just some vague memory from a high school history class. It is well-worn metaphoric shorthand for any defensive measure firmly believed to provide excellent protection, but that is in fact quite useless. Actually, worse than useless—because building a Maginot Line creates the complacency of a false sense of security.

There was a time, of course, between the two world wars, when the Maginot Line was more than a phrase. It was a reality of excavated earth, reinforced concrete, and powerful artillery: "an immense project comprising l00km of tunnels, 12 million cubic metres of earthworks, 1.5 million cubic metres of concrete, 150,000 tons of steel and 450km of roads and railways." [1] The brainchild of French Minister of War André Maginot, it was built between 1928 and 1938 along much of France's eastern border and cost 3 billion francs [2] in the 1930s, which is about 3.7 billion 2017 U.S. dollars. The finished fortification complex had 589 principal structures above ground plus some 5,000 small detached blockhouses. Connecting many of the principal buildings were subterranean tunnels, barracks, and storage facilities. It was an ambitious marvel of military engineering.

What did the people of France get for their $3.7 billion investment?

On the face of it, very little. The conquest of France in 1940 took just forty-six days. When the nation surrendered, it had lost not only the so-called Battle of France, but World War II itself. The German invaders suffered about 163,676 casualties, killed and wounded, but French military casualties totaled 2,260,000, killed, wounded, or made prisoner. [3]

Ray A. Rothrock is CEO and chairman of RedSeal Inc., a company providing enterprises with a network modeling and risk scoring platform that measures and improves resilience to cyber events and network interruptions. He is partner emeritus of Venrock; and a member of numerous boards including CheckPoint Software, U.S. Department of Energy GAIN, Roku, Inc., Tri Alpha Energy, Inc., Team8, and UTIMCO, a $40B public endowment for the University of Texas and Texas A&M University. He also is a member of the Corporation of the Massachusetts Institute of Technology.

In 2017, Ray led conversations at the Milken Institute Global Conference, the SXSW Conference, and the NACD Global Board Leader's Summit. He also participated in the 2015 White House Cybersecurity Summit. Ray holds a BS in Nuclear Engineering from Texas A&M University, a MS in Nuclear Engineering from the Massachusetts Institute of Technology, and an MBA with Distinction from Harvard Business School.

On the face of it, the Maginot Line represents a spectacularly poor return on investment (ROI) and richly deserves to survive in language as mocking shorthand for a disastrous monument to a collective national posture of heads-in-the-sand.

What served for many years after World War II as a durable label for any instance of delusional defensive strategy has become in the digital age an Internet meme signifying head-in-the-sand cybersecurity. A recent Google search on the phrase "Maginot Line cybersecurity" produced dozens of articles with titles like "Cybersecurity's Maginot Line," [4] "Don't Build a Maginot-Line Cybersecurity Defense," [5] "No More Cyber Maginot Lines: We Need to Hunt Down Hackers Before They Strike," [6] and "Avoiding Maginot Line Mentality: What False Assumptions Underpin Current Cyber Security Strategies?" [7]

You will find some thoughtful and valuable ideas in this "Maginot Line" genre of cybersecurity writing. Go ahead and skim. But I must caution you: all of the articles and reports in this Maginot Line group suffer from the same flaw. All base a complex argument on the same unexamined meme. The historical, strategic, and doctrinal realities behind the Maginot Line meme reveal what serious military historians have long understood, but nobody else has bothered to investigate. The Maginot Line has been getting a bad rap.

Now, before I set down another word, let me assure you that this article is not really about the Maginot Line. It is about the single most critical mistake most businesses make when they set their cybersecurity spending priorities: prioritizing security over resilience. [8] Before I define both security and resilience, it really will help if we understand the reality behind the Maginot Line meme. Allow me, then, just a few more sentences on this episode of military history.

The Maginot Line's champion and namesake disclaimed any intention of building in France the equivalent of the Great Wall of China "Instead," André Maginot wrote, "we have foreseen powerful but flexible means of organizing defense, based on the dual principle of taking full advantage of the terrain and establishing a continuous line of fire everywhere." [9] Maginot had served as a sergeant during World War I and was awarded the *Médaille militaire,* France's highest military honor. [10] This minister of war was neither a bureaucrat nor a theorist. He was a combat veteran with real-world experience, who understood that no passive wall would keep out a determined enemy. And so, the Maginot Line was not a wall, but a coordinated set of active defenses designed not to stop an army, but to slow it down by killing as much of it as possible. Its purpose—its true purpose—was to create strategic and tactical opportunities for organizing not just a defense, but effective counterattacks. Military historian Julian Jackson, wrote, "the Maginot Line had never been conceived as a ... Great Wall of China sealing France off from the outside world. Its purpose was to free manpower for offensive operations elsewhere." [11]

It pays to parse Professor Jackson's final sentence. The "purpose"—the top priority—of the Maginot Line was not defense but offense to "free manpower for offensive operations." The Line's defensive function—its security function—was secondary to its offensive function, which we can call resilience. The French plan never assumed that the Maginot Line was an impenetrable firewall. It was, rather, what military theorists, as well as warfighters, call a force multiplier. Force multipliers "work to optimize force capabilities ... The concept of force multipliers is a key element of U.S. military doctrine that asserts we can fight with limited resources and win." [12] Used correctly—not as a security device (a "wall"), but as a force multiplier (a device to enhance resilience), the Maginot Line should have been instrumental in defeating the Nazi invasion of France:

> The true flaw in French military strategy during the opening days of World War II lay not in reliance on the Maginot fortifications but in the [French] army's neglect to exploit the military opportunities the Line created. In other words, the border defense performed as envisioned, but the other military arms supported it insufficiently to halt the Germans. The French Army squandered the opportunity not because the Maginot Line existed but because they failed to utilize their own defensive plan properly. [13]

Instead of following the plan, which was to prioritize resilience to enable an effective offensive operation against the invaders, the French commanders chose instead to hunker down behind the Line, as if it were an inert and impenetrable wall. *The French leadership prioritized security over resilience.*

For anyone charged with protecting digital networks and the data that flows across them, the strategic error of the French commanders in 1940 is the real lesson behind the shallow and misleading Maginot Line meme: *Understand cybersecurity as more than*

sec-urity. Effective cybersecurity plans for, provides for, and executes on both security and resilience—with the greater priority always given to resilience: the ability to fight back, quickly and effectively.

André Maginot and the other original planners of strategic doctrine around the line of fortifications that was posthumously named for him understood that fortifications by themselves will not stop an invasion, but they can facilitate defense through a counteroffensive. These men would have understood former James B. Comey (at the time FBI director) when he told CBS *60 Minutes* in October 2014, "There are two kinds of big companies in the United States … those who've been hacked … and those who don't know they've been hacked." [14] They would have understood that no "wall" is sufficient to prevent penetration of a nation or a digital network. They would have understood that, while security is a necessary, even essential, tactic, it is not a sufficient strategy. It must be applied in coordination with resilience.

We don't know if Maginot and his colleagues were familiar with Sun Tsu's ancient maxim that "a victorious army wins its victories before seeking battle; an army destined to defeat fights in the hope of winning." [15] We suspect Director Comey was familiar with it. In any case, the maxim applies to both France in 1940 and digital networks today. The Maginot Line was planned as part of a war-winning strategy on the assumption that nothing could absolutely prevent an invasion. The failure of the Line was due not to a faulty plan, but to the substitution of the mere "hope of winning" for the faithful execution of what was a reasonable plan. Concerning cybersecurity, Comey's statement implies that no defensive measure—no mere security approach—can absolutely prevent a breach. The proof of this is that the battle against hacking has already been lost. If you don't know that your organization has been hacked, it has been hacked without your knowing it. Since security is therefore insufficient (though necessary), you need a means of digital warfighting that is effective against the attacker you know as well as the attacker you do not know. You need a means of effectively responding to the penetration that has already occurred, the breach that is currently in progress, and the breach that will inevitably happen.

The most profound implication of Comey's remark is that those of us responsible for protecting networks need to understand the basic difference between security and resilience. Security is analogous to the "wall" function of the Maginot Line. It is about preventing an attack. This is a necessary function and a laudable objective, but it is insufficient for the same reason that former Secretary of Homeland Security Janet Napolitano gave (when she was governor of Arizona in 2007) for not building a border wall to stop illegal immigration: "As I often say, 'You show me a 50-foot wall, and I'll show you a 51-foot ladder.'" [16] It is not sufficient to hope that a wall, security alone, will bring victory. Resilience, the other component of effective cybersecurity strategy, neither offers nor depends upon hope. Resilience is, in fact, creatively pessimistic in assuming that a large number of cyberat-

tacks will inevitably be directed against any and every organization, that security devices will inevitably fail to stop a significant fraction of those attacks, and that management's top cybersecurity priority should be reducing the volume and severity of damage and loss as well as staying in business or on mission during a breach. It is in such a reduction of impact that we find the likelihood not only of survival and recovery but of even continuing to operate without interruption. Resilience is about standing up to do business while fighting back and recovering.

A cybersecurity strategy that prioritizes resilience includes, at minimum, six elements:

1. **It intelligently assesses data assets for protection.** Resilience must be framed not as an IT department security strategy but as a whole-enterprise business strategy. Security imperatives do not necessarily coincide with the imperatives of resilience. For example, arbitrarily limiting customer access to data may increase security, but it also impedes the ability to do business. A hobbled organization is a less resilient organization in that it is a step closer to failure. Resilient organizations strategically prioritize access by assessing data assets in terms of network accessibility, critical sensitivity of information, value of proprietary intellectual property, and customer need-to-access.

2. **It focuses on performance outcomes rather than infrastructure protection.** Resilient organizations devote the greatest resources to protecting what keeps them operating—that is, performance for "customers" (defined as everyone the organization serves) and achieving the assigned mission. Infrastructure exists to enable performance, not vice versa. Resilient strategy always balances performance against security.

3. **It prioritizes detecting breaches and responding to them.** Resilience assumes the reality that bad things are happening. Security seeks to prevent bad things from happening. The first engages a reality. The second takes certain defensive steps in the hope of evading or postponing that reality.

4. **It creates understanding of how data flows into, out of, and through the organization's networks.** Without this understanding, it is impossible to apply appropriate and effective controls on data access. In contrast to resilience, the imperative of security is to control (in other words, to restrict) the flow of data.

5. **Resilience engages the entire organization.** Security strategies tend to focus on IT technology. Resilience engages the people who use technology. Its objective is to create an organizational culture of resilience, which enhances both security and the capacity to stand up under attack, continue operating during a breach, and rapidly recover in the aftermath.

6. **Most of all, resilient strategy declines to waste resources on defending perimeters in the "hope of victory."**

In 1940, France had a perimeter to defend. Today's extensively connected, intensively interactive digital networks ultimately have no perimeters. Today, attacks come from everywhere, from without and within. The multiplicity and complexity of connections present both unprecedented opportunities and unprecedented risks. Every organization understands that the quality of its product is only as good as the quality of its supply chain. If you're in the business of making lemon meringue pies, your pies can never be better than what your lemon suppliers sell you. By the same token, an organization's network is only as secure as the networks with which it connects.

World War II may have been the last war with definable fronts—distinct perimeters. Perhaps, then, the stewards of today's digital networks are better served not by the 1940s metaphor of the Maginot Line, but by the more recent reality of insurgent warfare. During the 1960s and 1970s, the Vietnam War forced the U.S. military to transform itself into an organization capable of fighting armed conflicts in battlespaces without fronts. This is the situation for today's digital network users and managers. The complexity and multiplicity of today's Internet, which includes the vast network of the Internet of Things (IoT), forces organizations to discard the notion of any network "perimeter" to defend. As University of Cambridge computer scientist Robert Watson has put it, "The default assumption is that everything is vulnerable." [17] The only realistic response to this new reality is for digitally transformed organizations to create the necessary resilience to sustain high performance while identifying and neutralizing intruders both coming and arrived.

NOTES

1. William Allcorn, *The Maginot Line,* 1928-45 (London and New York: Oxford University Press, 2003), 9.

2. Robert Kuttner, "The Economic Maginot Line," *The American Prospect* (August 11, 2011), http://prospect.org/article/economic-maginot-line.

3. Micheal Clodfelter, *Warfare and Armed Conflicts: A Statistical Reference to Casualty and Other Figures, 1500-2000* (Jefferson, NC: McFarland and Company, 2002), 489.

4. Fire Eye, "Cybersecurity's Maginot Line: A Real-world Assessment of the Defense-in-Depth Model," https://www2.fireeye.com/real-world-assessment.html.

5. Eric Holdeman, "Don't Build a Maginot-Line Cybersecurity Defense," *Emergency Management* (March 14, 2016), http://www.govtech.com/em/emergency-blogs/disaster-zone/dont-build-a-maginot-line-cybersecurity-defense.html?flipboard=yes.

6. Nate Fick, "No More Cyber Maginot Lines: We Need to Hunt Down Hackers Before They Strike," *Defense One* (June 5, 2016), http://www.defenseone.com/ideas/2016/06/no-more-cyber-maginot-lines-we-need-hunt-down-hackers-they-strike/128823/.

7. Editorial Team, "Avoiding Maginot Line Mentality: What False Assumptions Underpin Current Cyber Security Strategies?" *CrowdStrike* Blog (April 14, 2015), https://www.crowdstrike.com/blog/avoiding-maginot-line-mentality-what-false-assumptions-underpin-current-cyber-security-strategies/.

8. In a survey of 200 corporate CEOs conducted by RedSeal, Inc., in September 2016, 50 percent reported prioritizing "keeping hackers out of the network" while "just 24 percent were concerned with building capabilities to deal with hackers who have successfully breached their network's perimeter defenses." (RedSeal, "Cybersecurity Perception Survey," conducted by Finn Partners, September 2016; "RedSeal CEO Survey: Summary & Key Findings," https://www.redseal.net/wp-content/uploads/2016/12/RedSeal-CEO-Survey-Executive-Summary.pdf, 1.

9. Charles River Editors, *The Maginot Line: The History of the Fortifications That Failed to Protect France from Nazi Germany During World War II* (N.p.: Charles River Editors, n.d.), Introduction; Kindle ed.

10. Laura Lee, *The Name's Familiar II* (Gretna, LA: Pelican Publishing Company), 226.

11. Julian Jackson, *The Fall of France: The Nazi Invasion of 1940* (New York: Oxford University Press, 2003), 27.

12. Major David S. Powell, Field Artillery, *Understanding Force Multipliers* (Fort Leavenworth, KS: School of Advanced Military Studies, United States Army Command and General Staff College, 1990), http://www.dtic.mil/dtic/tr/fulltext/u2/a234153.pdf, 1.

13. Charles River Editors, Introduction; Kindle ed.

14. James B. Comey, quoted in Scott Pelley, "FBI Director on Threat of ISIS, Cybercrime," *60 Minutes* (October 5, 2014), http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/.

15. Samuel B. Griffith, trans. and ed., Sun Tzu, *The Art of War* (London and New York: Oxford University Press, 1963), 87.

16. Glenn Hurowitz, "Who Me a 50-Foot Wall, and I'll Show You a 51-Foot Ladder," *Grist* (November 21, 2008), http://grist.org/article/napolitano-knows/.

17. The Economist, "Why everything is hackable," *The Economist* (April 8, 2017), 69.