



How to Survive a Cyber Pearl Harbor

Ronald P. Loui, University of Illinois at Springfield

Terrence D. Loui

An examination of parallels between the “Day of Infamy” and a major cyberattack reveals lessons for organizations about vulnerability, the nature of survival, and the tenets of protection that can help boost resilience against hackers and other cyberthreats.

When drawing attention to cyber vulnerabilities, there are many reasons to refer to a cyber Pearl Harbor. It is a reminder of the risks of feeling invulnerable and of being unprepared for—even complacent toward or doubtful of—an attack of this scale and nature. Pearl Harbor also represents the vulnerability of a system’s defense, particularly when faced with a paradigm shift. It is a clear symbol of the kind of unimaginable attack executed by distant foes thought incapable of such destruction.

December 7, 1941, was indeed a “Day of Infamy.” Although younger IT professionals might not attach as much significance to the date as the generation before them, most understand that it was a predecessor to 9/11 and marked the US entry into the Pacific Theater of World War II. Most also know it as a dreadful day for the US Navy (USN) because thousands of lives were lost, and many Imperial Japanese Naval (IJN) objectives were met.

Yet when people think of Pearl Harbor, they often fail to understand one simple fact: the Japanese victory was incomplete. The IJN’s two aerial attack waves missed some important strategic targets. US Naval fuel reserves remained intact, pampered under Red Hill, three miles north of the harbor lochs. The US Army Air Forces (USAAF) air-to-air scores were 8-0 against Japanese ground-attack planes, and possibly 8-1 against the vaunted Mitsubishi A6M Zeros. Overall, more US planes were lost to friendly fire than to air-to-air combat, and the Japanese air superiority fighters returned to their carriers after a short time.

Thus, inasmuch as Pearl Harbor symbolizes a surprise attack, it also provides key lessons for attack survival.

After the second wave, the Japanese realized that USN defenses had become too well organized for the attack to continue. Further, it would be too much of a risk, not knowing the location of the USN carriers, to remain in distant waters rather than to withdraw. Arguably, if US

search planes had located the Japanese carriers by early afternoon, the attackers' victory might have turned into a tactical loss on that very day. In today's cyber engagements, the task of finding the perpetrators is also difficult.

As with most cyberattack scenarios, when contemplating the impact of an electronic Pearl Harbor, we must consider primary command-and-control effects, secondary effects on operations and infrastructure, tertiary effects on institutions and economies, and the morale of a nation. A number of useful analogies within this scenario can be translated into lessons

on paper, it led to disaster. Targets in such close proximity effectively increased torpedo and bomb accuracy and allowed many first-class targets to be included as collateral damage from other targets.

Lesson: Collocation enables multiplicative damage

This lesson has relevance today because of the shared configuration in computing: a single platform, the same OS, one middleware approach, one compiler or database vendor, and one administrator password or a root account to open them all. When many

Commercial databases can be mirrored in MySQL databases, or even nonrelational stores, which is how our Cleveland Clinic group endured server and network outages. Instead of insisting that Java be used everywhere, it might make more sense to argue for Python, Ruby, and C# on the grounds that they add logical distinctions. It could be anathema to organizations that prefer official versions and standardized software, but survivability suggests that personnel are better off using multiple browsers, multiple search engines, multiple mail clients, different URLs for replicated webservices, and so on. The real push should be for varying configurations.

An example of multiplicative damage is a 1994 attack that started in our university's physics department and continued through shared accounts to other cycle servers. The attack spread to dozens of engineering machines through the mail server, then interrupted hospital operations through a hundred similarly configured Solaris Network File System (NFS) workstations. Fast forward 20 years later, and collateral damage is two orders of magnitude larger: the Iranian cyber-attack on Saudi Aramco brought down 30,000 computers because of a single vulnerability in the master boot record disk in Windows System32 machines, which were too similarly specified and thus subject to the Shalmoon machination.¹

Many have called for producing logical variation automatically. DARPA's 2014 program for transformations of program binaries is an example of an attempt to increase attack immunity by building additional heterogeneity into systems post hoc.² DARPA lists as a 2011 accomplishment, "a novel compiler that generates distinct binary

POSSIBLY THE MOST IMPORTANT TRANSFORMATION FROM KINETIC WAR TO CYBER WAR: POSITION IN SPACE IS LOGIC IN CYBERSPACE.

for cyber warfare, although even the best analogies have their limits. The lessons that follow are those we deem most relevant.

KNOW THE DANGER OF SHARED SPACE

First, what went wrong at Pearl Harbor? The planes were famously parked wingtip to wingtip at the major air fields, under the orders of General Walter Short, except for a line of P-36s at Wheeler Air Force Base (AFB), which had been removed the night before. The ships were juxtaposed, under the orders of Admiral Husband Kimmel, bottled up in a shallow harbor and in dry dock. While this appeared impressively secure

machines share program logic or a network, a single exploit can open them to attack in parallel. When all machines are running related Java versions, one bug in one library exposes them all at the same time.

In cyberspace, two computers could be miles away, but if they are connected, and use the same mail reader or Oracle release, they can be attacked simultaneously. The replication and duplication that makes it possible to manage a fleet of machines is the same replication and duplication that makes them go down in one event.

This is possibly the most important transformation from kinetic war to cyber war: position in space is logic in cyberspace.

files for every new compilation of the source code.” Such individualized computer immune systems date at least to 1997.³

Different weapons systems are like different computing platforms. The USN submarines and docks at Pearl Harbor survived the attack, and were of course instrumental in winning the Pacific War. Similarly, different platforms will have different prospects for surviving a cyberattack.

BE REASONABLE ABOUT INTERNAL SECURITY

On 7 December, sabotage from local citizens was a concern, and lockdown assuaged the commanding officers’ reasonable fears of this threat. But locking down the airfields famously prevented rapid effective response when the airfields were under enemy fire. Ammunition and fuel were separated from planes, which were separated from pilots, each separately secured.

Lesson: Internal security retards response under attack

An inconvenient fact is that the first US planes in the air were those that had been parked in violation of the airfield’s security policy. The P-36s that 1st Lieutenant Lew Sanders and his wing flew out of Wheeler AFB were parked separately the night before, essentially because the secured parking area was full.

Imagine dozens of cyberwarriors trying to respond to an attack but locked out by the failure of internal controls, such as password authentication—the electronic equivalent of a locked hatch on a sinking ship.

Or imagine a network engineer trying to patch and reconfigure quickly, to put servers out of reach, possibly on a different LAN, only to fail

because of an overly aggressive data loss-prevention firewall that blocks unknown ports and IP ranges—the electronic equivalent of being locked in by a harbor torpedo net. As Lieutenant Francis Gabreski recalled, “The last hangar held all the refueling trucks, completely filled with gasoline. We tried to move them but found no keys.”^{4,5}

A cyberwarrior with powerful resources can often restore breached machines through quick and clever action; it would be foolish to discount the possibility of heroic human initiative. Quick action is critical when

and providing no workarounds can lead to catastrophe.

CONNECT ON DEMAND, NOT BY DEFAULT

The existence of a large number of computers does not require that machines be connected in a highly exploitable way. It has been the desire of commercial computing companies to provide functionality to corporate and casual users who, to be frank, can be naive and lazy. Marketing to these consumers has led to licentious design and engineering: docking, tethering, unsupervised wireless roll-



IMAGINE DOZENS OF CYBERWARRIORS TRYING TO RESPOND TO AN ATTACK BUT LOCKED OUT BY THE FAILURE OF INTERNAL CONTROLS.

the rules constraining responses are exactly the rules being exploited and co-opted by the attackers. Some of this rationale appears to be motivation for the Air Force Rome Labs’ solicitation for agile cyber defenses.⁶

A systems administrator who must sudo (superuser do) for every sbin command can be like a P-36 Wheeler pilot who is ready to fly, but watches his plane sit in flames.

A recent report in an AFCEA (Armed Forces Communications and Electronics Association) *Signal* article reported this phenomenon: “all too often, the security team is beating the administrators over the head to ... use more security tools.”⁷ Having many doors that lock is a good idea, but locking too many doors

over, bluetooth and other near-field communication, and portable media devices that cross firewalls through physical transport. Hackable cloud services or cloud connections, public Wi-Fi, and an Internet of Things are likely to lead to much more dangerous failures. Because commercial computing has been prioritizing sales and access over security, too many applications have programmable environments for executable macro and attachment exploits.

Lesson: Network but don’t tether and dock together

Pearl Harbor showed us that a fleet can share a base of operations, maintenance, and command, but not

necessarily dock together and sleep together. Massing of force can be good, but swarms can be neutralized or eliminated en masse; there might be other ways to concentrate firepower without sharing vulnerabilities. The coveted carriers were based at Pearl Harbor but operated independently of the ships tethered and sunk at Ford Island: Fleet Admiral William Halsey Jr.'s, *Enterprise* carrier group, with three cruisers and nine destroyers, was at Wake Island; *Lexington* and her eight escorts were near Midway Island; and the *Saratoga* was being fitted with an aerial complement at the Naval Air Station in San Diego.

It is important to manage connectivity, not just maximize it. Many of today's conveniences—remote access through virtual desktops, remote updates, and networked file systems—are today's battleship row: "What the USS *West Virginia* had to actually guard itself against was collateral damage from the explosion at the USS *Arizona*" (www.pearlharborinhawaii.com/usswestvirginia.html).

CROSS-TRAIN SYSADMINS

Some of what went right for the US on 7 December happened by accident. P-36s were being replaced with P-40s. P-36s were good at diving onto low-flying formations, and P-40s were more controllable in a dogfight. Both kinds of abilities were needed. Many of the pilots in P-36s that day were originally assigned to P-40s and vice versa, but all pilots had been trained on both planes.

Cross-training system administrators (sysadmins) is the direct analogy. Many IT departments train their first responders to know all the important systems because they often are

on call to cover late-night and weekend help requests. But very few IT departments within a large organization have shared coverage agreements or training with other, related IT departments in the same organization. One sysadmin and his staff serves one group; another sysadmin and her staff serve another; information about resources and requirements is shared only by accident.

Lesson: Cross-training enables flexible response

Contrast this with a squadron of pilots that can jump into another squadron's planes at any time: each squadron already understands how to coordinate and communicate, and can provide air superiority, pursuit, patrol, or reconnaissance as needed.

[Pilot Lt. John Leroy] Dains flew three missions on the morning of 7 December 1941 The first two missions were flown in a P-40 type airplane, and the third mission in a P-36 type airplane. (From the Silver Star citation text for Lt. John Leroy Dains; www.homeofheroes.com/members/04_SS/2_WWII/citations/citatons_Dec7.html.)

RESIST PRESSURE TO CONSOLIDATE

IT managers are routinely pressured to consolidate to control costs. But in doing so, they ignore the less obvious cost of reducing system robustness and survivability. Some preach that maximized utilization is maximum efficiency, but the tradeoff is no headroom for bursts, no room for failure or damage, no room for best-practices experimentation, and no flexibility to seize unanticipated opportunities or to perform additional training. It

means no room to respond to the stress induced by an adversary.

Lesson: Diversify systems, preserve headroom, and avoid relying on utilization as the sole metric

DARPA's Dan Kaufman shared his thoughts about preserving system heterogeneity in an era of consolidation. Excerpts from a 2011 video of Kaufman describing DARPA's cyberanalytical framework (www.youtube.com/watch?v=RyH6BrEPkZk) illustrate the tension between the pressure to consolidate and the recognition that heterogeneity has compelling advantages.

To improve information security and reduce overall IT operating costs, we're going to put everyone on the same system. [T]hose are two radically different things. ... I buy ... that it will save us money. [To] somehow make this wild jump that somehow we're all more secure, I don't see any foundation for it.

We heard a lot about heterogeneous systems; we all know there are huge advantages to them. But the cry you hear from the IT managers is, well they're inherently unmanageable. [I]t's a DARPA question to ask ourselves 'why?'. These things aren't written in stone; they're just things we've accepted over time. And so we try to drive our programs to break these false choices.

A three-way platform mix is much more robust than a single platform against adversarial action because the probability of a successful attack on all three is the product of the probability of successful attack on each. To

achieve a high degree of confidence in the ability to disable a system, an attacker must plan for a significantly higher probability of success against each component.

For example, with a 90 percent chance of a successful attack against each independent channel, a one-channel system survives 10 percent of the time; a two-channel system, 19 percent; a three-channel system, 27 percent; a four-channel system, 34 percent; and a five-channel system, 41 percent.

Many students of traditional engineering subjects are taught to think this way, but IT has developed with a different culture. Computing culture has always been about “winner take all” and “shiny and new.” But one way to increase heterogeneity with little cost is simply to stage upgrades.

Considering a potential insider threat from a disgruntled former sysadmin, it might be wise to retain older systems with existing personnel as a second pathway. If you keep the older sysadmin instead of firing or demoting that person, you won’t have to change all the locks. At the very least, older systems have proven functions and well-understood engineering.

UNDERSTAND IMPERFECTION

Oahu had 10 functioning airfields, and 9 were in flames in the first hour of the attack: Kahuku Point Airfield, Kaneohe Naval Air Station, Bellows Field, Hickam Field, Honolulu Naval Air Station/John Rodgers Field/Naval Air Station Barbers Point, Ford Island, Wheeler AFB, Ewa Marine Corps Air Station, and Dillingham Mokuleia Airfield. Each name conjures images of planes burning on the ground.

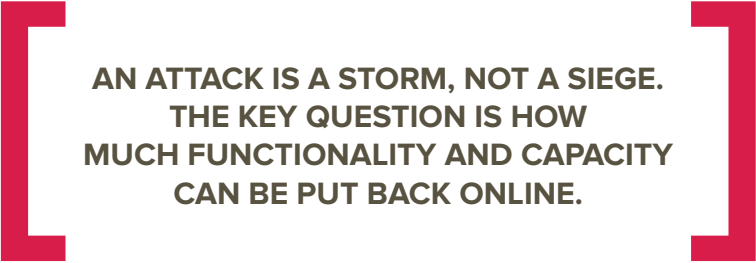
The tenth airfield, Haleiwa, was an emergency landing strip, consisting of a grass airfield with no hangars

that apparently did not appear on the Japanese pilots’ maps. From that airfield, several pilots took to the air with impressive results.

Haleiwa didn’t cost the military much at all because its operational standard was far below the others. Indeed, those on temporary duty at Haleiwa had to bring “their own tents and equipment.”⁸ Nevertheless, the airfield had existential capacity for a critical two hours when nine primary airfields were down.

for a 1-Kbyte file. Depending on load balancing, a healthy server might process 100 requests per minute externally and 10 per minute internally, which would put the peak rate several orders of magnitude above the existential requirement. Similar ratios can be observed for network and disk bursts compared to averages, simply by watching performance meters.

Because of spectacular gains in computing capability each year,



**AN ATTACK IS A STORM, NOT A SIEGE.
THE KEY QUESTION IS HOW
MUCH FUNCTIONALITY AND CAPACITY
CAN BE PUT BACK ONLINE.**

Lesson: Decimated capacity can still support normal function

Around 10 percent of USAAF aircraft made it into the air that day, but, in combination with ground antiaircraft, they provided enough support to regain control of island skies within hours. Of 402 planes stationed on the ground, 42 planes made 81 take-offs.⁹

Like the defense of Oahu, most computer systems are deployed with overcapacity, specifically to cope with bursts.

For a computer or communications system at peak, the resource demand is often 100× to 1,000× the normal load. For example, on the University of Illinois at Springfield’s cyber range (a testbed for malware, viruses, and the like), we measure just 5 percent CPU utilization on an old 1-GHz web-server with 2,000 Apache2 listeners serving 50,000 requests per minute

removing 90 percent of capacity might be the equivalent of returning systems to the state of the art 5 or 10 years ago, which is not such a dire loss.

Cyberattacks that target systems, as opposed to data, might be hard to press to completion; such attacks can do extensive damage yet not damage everything required to incapacitate the system.

Lesson: Downtime is not so bad if recovery is quick

The impressive air-to-air score did not reverse the IJN victory, but once Wheeler AFB was back in operation, it was enough to bring the attack to an end by noon.

A sysadmin could hear this as “within the first hour, two firewalls were back up, then all the essential services, and by noon, our mirrored

databases were online and we were doing forensics and attribution.”

The Pearl Harbor attack could not be sustained, especially after such distant force projection (projecting force at a great distance, usually with a carrier or strategic bomber). Cyberattacks are often considered the ultimate form of distant force projection, but with different properties. They might be equally hard to sustain. A denial-of-service attack cannot be projected across many hops without eventual diminution; it is a storm, not a siege. Machines get restarted with fresh images and IP addresses get blacklisted. Mitigation strategies take hold.

Full restoration and reconfiguration might take time, but the key question is how much system capacity and functionality can be put back online. The real story was that Pearl Harbor itself was back at full capacity as a US naval base within weeks of the attack.

Lesson: Hardware slaughter is not strategic victory

In the near future, restoration of information services might be done so quickly that downtime could become a secondary consideration. The well-prepared and well-provisioned sys-admin can often just unplug a compromised machine, putting a recent copy in its place. Virtualization and better firewall scripting could soon be more helpful in this context.

ASSESS DAMAGE FUNCTIONALLY, NOT NUMERICALLY

Particularly relevant to today's cyber landscape is the sheer inventory of what can be damaged in an attack. Many devices can be expected to go

down instantly, and the psychological impact is likely to be severe.

But today's surviving device is capable, like a surviving carrier group. In fact, some damage can be a blessing in disguise. The torpedoed battleships were so old that they would have been fuel-wasting hulks during the quickly modernizing Pacific campaign.

The proper place for damage assessment is in the secondary effects. Assessment might entail asking questions such as

- › What did the adversary do during the outage? Victory at Pearl Harbor was temporary and even debatable. No Japanese boots marched on US soil. The IJN never projected meaningful force on the West Coast.
- › What did the clients actually lose during the downtime or intrusion? Even a fully functioning USN flotilla could not have altered the fate of the British *Repulse* and *Prince of Wales*, three days later on the other side of the ocean.
- › Were the right decisions made for a proportional and distinctive response to the proper parties, with a view toward long-term outcomes?

President Franklin D. Roosevelt used the Pearl Harbor attack to move the nation to war, as he deemed engagement necessary in Europe. But war in the Pacific was as much an emotional response as rational response:

Pearl Harbor may well have been ... a disaster. It clearly was ... for the attackers. [But it] propelled the [US] heedlessly into a long,

*ghastly war in Asia when continued containment ... might have rolled back the Japanese empire at lower cost to all.*¹⁰

Beyond the secondary effects, what is the sociopolitical damage? Despite massive morning losses, who won the war? Most understood, even shortly after the attack, that Pearl Harbor was one of history's biggest strategic blunders. The attacking nation had gambled on US capitulation in the face of shock and awe, and they gambled wrong. But the response could also be appraised critically. One of the pitfalls associated with cyberattacks is the potential to respond reactively, without specificity or proportionality, or without considering all options.

The Japanese surprise attack on Pearl Harbor could have gone the other way if US carriers, fuel reserves, and national morale had figured differently. It is the same with massive surprise cyberattacks. Systems must be well engineered to survive. Oahu's air defenses were well engineered despite command and intelligence blunders.

There can be shocking numerical losses in cyberspace. But in properly engineered systems that have multipath systems with logical diversity, mirroring, redundancy, and sufficient independence, those losses will be syntactic, not semantic.

Pearl Harbor is actually an excellent example of shocking paper losses that amounted to nothing in strategic terms. The deaths of servicemen and civilians are mourned, but the US survived the attack. Those who can transform the lessons of the past should

likewise be positioned to endure a cyber Pearl Harbor.

Aside from massive surprise attacks, many other cyberthreats are possible, and might well require different security considerations. Still, Pearl Harbor persists as a subject of national interest, as evidenced by the 1970 film *Tora, Tora, Tora*; the auspiciously timed 2001 film *Pearl Harbor*; and two PBS documentaries, *The War and The Roosevelts*.

What would an inspection of today's large computing systems reveal? Would it uncover vulnerabilities that would be easily exploited in a massive attack, or have the lessons of Pearl Harbor been learned and translated into resilient systems? Hopefully, IT managers have embraced heterogeneity and avoided collocation, resisting the philosophies of General Short and Admiral Kimmel, who lined up rows of airplanes wingtip to wingtip and anchored battleships in a tight line of neat, matched pairs. ■

ACKNOWLEDGMENTS

Terrence D. Loui died before this article was published, but together we conceived this article to honor our high school computer programming teacher, 2nd Lieutenant Henry Wells Lawrence. Mechanic Gordon H. Sterling famously took to the air in Lawrence's plane and was shot down, the only US air-to-air loss. Lawrence took off in a different plane later that morning.

REFERENCES

1. "Saudi Aramco Cyber Attacks a 'Wake up Call,' Says Former NSA Boss," *Infosecurity News*, 8 May 2014; www.infosecurity-magazine.com/news/saudi-aramco-cyber-attacks-a-wake-up-call-says.
2. Defense Advanced Research Projects Agency, *Cyber Fault-tolerant Attack*

ABOUT THE AUTHORS

RONALD P. LOUI is an assistant professor of computer science at the University of Illinois at Springfield. His research interests include cyberwarfare, artificial intelligence, and systems security and performance. Loui received a PhD in computer science and philosophy from the University of Rochester, and was a postdoctoral Fellow at Stanford. He is a member of IEEE and a founding member of the military technology section of the *Harvard International Review*. Contact him at r.p.loui@gmail.com.

TERRENCE D. LOUI was a civilian contractor with a top-secret clearance and one of the earliest network security and support engineers at the Defense Communications Agency at Wheeler AFB (DCA-PAC), which later became the Defense Information Systems Agency (DISA-PAC). He was a graduate of Champlain University and the Punahou School in Honolulu, and an avid student of Pearl Harbor military history.

- Recovery* (CFAR), 2014, solicitation no. DARPA-BAA-14-64; www.federalgrants.com/Cyber-Fault-tolerant-Attack-Recovery-CFAR-48363.html.
3. S. Forrest, S.A. Hofmeyr, and A. Somayaji, "Computer Immunology," *Comm. ACM*, vol. 40, no. 10, 1997, pp. 88–96.
4. F. Gabreski, *Gabby: A Fighter Pilot's Life*, Orion Books, 1991.
5. W.J. Horvat, *Above the Pacific*, Aero Publishers, 1966.
6. Department of the Air Force, *Capabilities for Cyber Resiliency*, solicitation no. BAA-RIK-14-07, 2014; <http://contract-opportunities.insidegov.com/1/252160/Capabilities-for-Cyber-Resiliency-BAA-RIK-14-07>.
7. G.I. Seffers, "Shifting Tides of Cyber," *AFCEA Signal*, 1 July 2013, pp. 35–37.
8. D.M. Goldstein, K.V. Dillon, and J.M. Wenger, *The Way It Was: Pearl Harbor—The Original Photographs*, Potomac Books, 1995.
9. S.E. Morison, *The Rising Sun in the Pacific, 1931– April 1942: History of United States Naval Operations in World War II*, vol. 3, Little, Brown, and Company, 1948.
10. J. Mueller, "Pearl Harbor: Military Inconvenience, Political Disaster," *Int'l Security*, vol. 16, no. 3, 1991, pp. 172–203.



Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.