

Digital Blitzkrieg

Updating the Pearl Harbor Analogy and Combating it Multi-Domain Civilian Red Cells

Timothy S. Rosenberg, JD

The Flaw of the Digital Pearl Harbor

As anyone will tell you, on December 7, 1941, the Japanese navy launched a surprise attack against United States naval ships docked at Pearl Harbor. 50 years later, Winn Schwartau coined the phrase ‘electronic Pearl Harbor’ to refer to the potential for a similar surprise attack on our nation’s critical infrastructure through electronic or digital weapons. A quick troll of the internet will show anyone that while the press loves the term, there are few professionals happy with it. As the Crypt Newsletter puts it:

” in the real world, [digital Pearl Harbor] is a cue for the phrase “Watch your wallet!” since those wielding it are usually doing so in an attempt to convince taxpayers or consumers to fund ill-defined and/or top secret projects said to be aimed at protecting us from it.”¹

This author couldn’t agree more. The phrase has been over used and worn out and worse still, is fundamentally flawed. There are several primary flaws in the digital Pearl Harbor analogy:

1. The attack did not include any new technologies
2. The attack was one dimensional in scope and therefore the damage was not long lasting

New Technologies

According to the U.S. Navy’s website entitled ‘A Brief History of Aircraft Carriers’, the first U.S. carrier was the USS Langley. The Langley was converted from the collier USS Jupiter and placed into commission March 20, 1922.² The year prior, the Japanese launched its first purpose build aircraft carrier, the Hosho in 1921.³ By the time the attack on Pearl occurred, carriers had been around the U.S. Navy had been landing and launching aircraft off ships for nearly 30 years.⁴ Furthermore, the first use of carrier launched aircraft in battle was off the HMS Furious in July of 1918 against the German Zeppelin base at Tondern.⁵ In short, the Japanese carriers at Pearl Harbor did what carriers are supposed to do; project air power to targets you normally couldn’t reach from land based aircraft. While the target and timing may have been a surprise, the method of delivery and technologies used were nothing new.

¹ <http://www.soci.niu.edu/~crypt/other/harbor.htm>

² <http://www.chinfo.navy.mil/navpalib/ships/carriers/cv-hist1.html>

³ http://en.wikipedia.org/wiki/Imperial_Japanese_Navy#Interwar_years

⁴ 1910, Curtiss plane takes off from the USS Birmingham, and 1911, a Curtiss pusher lands on the USS Pennsylvania; <http://www.chinfo.navy.mil/navpalib/ships/carriers/cv-hist1.html>

⁵ http://en.wikipedia.org/wiki/Aircraft_carrier#Genesis

One Dimensional Attack

The attack on Pearl was intended to neutralize U.S. naval power in the Pacific. That being the case, the chosen targets and method of attack were ill suited toward that goal. According to several references, only three ships were permanently disabled. Furthermore, no attacks were made on the submarine pens, repair facilities or the headquarters building. All three of the U.S. aircraft carriers were likewise untouched as they were all absent. While the attack was nonetheless devastating from a casualty perspective, it made little strategic impact to the overall war in the Pacific. As evidenced by the short list of engaged targets, the Japanese attack was one dimensional; ships in the harbor. The attack shows no understanding of the interconnectedness of various dimensions required to keep a navy operational. If the goal of the attack was to create a U.S. navy without ships, then complete and utter destruction of the physical ships is only the starting place of the attack, not the end point. Every domain that is necessary to keep a ship afloat must be targeted. That means:

- Repair facilities
- Refueling depots
- Aircraft and submarines
- Command and control sites and personnel
- Any other facility even collaterally associated with the fleet:
 - o Personnel barracks and housing
 - o Training facilities
 - o Food storage sites

Failure to attack cross domains results in the ability for rapid recovery from the attack. Only three ships were permanently destroyed. Several others were back in operation within several months. The carriers and submarines were untouched. As the attack demonstrates; single domain attacks result in short term single domain victories, NOT sustained strategic impact. The United States ultimately won the war in the Pacific

The Digital Blitzkrieg – Multi-Domain Attacking

In studying the German Wermacht's Blitzkrieg through Western Europe, there has much (some would say too much) emphasis on the use of armor. As John Ellis states

“Of course, these armored forces did play a somewhat more important role in operations than the simple proportions might indicate, but it still has to be stressed that they in no way dominated the battlefield or precipitated the evolution of completely new modes of warfare.”⁶

While armor did play an important role, it did not, in and of itself, create a new strategic battlefield. What makes the Blitzkrieg an interesting case study for current trends is this; the Germans successfully blended advances in several divergent technologies into a new way of fighting war. Case in point is the seizure of the Belgium fortress Eben Emael in 1940.

⁶ Brute Force, John Ellis, 1990.

In William H. McRaven's book *Spec Ops: Case Studies in Special Operations Warfare Theory and Practice*, the author examined eight historical special operations missions in an attempt to identify the theory of special operations. Through the development of this theory, McRaven states "if we can determine, prior to an operation, the best way to achieve relative superiority, then we can tailor special operations planning and preparation to improve our chances of victory"⁷ What makes McRaven's theory applicable to the Digital Blitz analogy is the primary characteristic of special operations warfare; a small highly trained force engaging a larger, better armed force in a fortified position. This asymmetry is the perfect model for a digital blitz and no more so than the German seizure of the Belgium fort Eben Emael which was the spearhead to the Blitzkrieg across Western Europe.

As McRaven points out, Eben Emael was the largest fort in Europe and built to dominate a World War I battlescape. In 1940, a group of 69 men took and held this monolith protected by a group 10 times the size of the assault force.⁸ The attack had two firsts; the first use of glider aircraft in combat and the first use of shaped charges.⁹ The plan was simple, limited in scope, and surprising in nature. While the gliders were spotted prior to landing and even took direct fire, McRaven notes that the real surprise was the use of shaped charges which destroyed the armored casemates and cupolas at the fort within 20 minutes of landing. The fort was built to withstand direct assault. The defenders had interlocking fields of fire and believed the landed paratroopers to be little threat. It was the rapid destruction of their fixed defensive positions that was the surprise.¹⁰

This tactical portion of the Blitzkrieg illustrates the general model of the strategic Blitz; combining new technologies and new uses for old technologies to create a blended offensive strategy that achieves victory through speed, limited mission objectives, and innovation. This provides the basis for the Digital Blitzkrieg when combined with Arquilla and Ronfeldt's concept of swarming.

In the book *Networks and Netwars*, authors John Arquilla and David Ronfeldt define swarming as:

"a seemingly amorphous, but deliberately structured, coordinated, strategic way to strike from all directions at a particular point or point, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions".¹¹

Some key characteristics in swarming include:

- [the ability] "to coalesce rapidly and stealthily on a target, then disperse and redispense, immediately ready to recombine for a new pulse"¹²
- "may be most effective, and difficult to defend against where a set of netwar actors do not 'mass' their forces, but rather engage in dispersion and 'packetization.'"¹³

I would add one thing to the swarming concept and that is the multi-dimensional swarm or MDS. An MDS operates in similar fashion to a traditional swarm. Instead of a group of actors

⁷ *Spec Ops: Case Studies in Special Operations Warfare Theory and Practice*, William H. McRaven, pg 1

⁸ *Ibid.* pg 55

⁹ *Ibid.* pg 62

¹⁰ *Ibid.* pg 66

¹¹ *Networks and Netwars*, by Arquilla and Ronfeldt, 2001, pg 12

¹² *Ibid.*

¹³ *Ibid.*

aggregating from multiple directions to engage a target an MDS would involve multiple groups of actors aggregating from multiple directions to engage multiple aspects of a single target along a random variable attack schedule. As with many things, the definition is long, the example is easier.

Multi-Domain Attack Plan – The Digital Blitzkrieg

Let's say you wish to attack the United States. To do so in the physical realm would be costly in lives and materiel and stand little chance of success. Technology has given the United States dominance over the traditional fields of battle; land, sea and air. As with the Eben Emael example, when the old battle fields have been dominated, it is time to create a new battle field. Eben Emael was built along World War I technology and strategy; direct assault by air and infantry. The Germans created a new battle field, the roof as accessible by glider. Furthermore, they used new tools to conquer the old. The casemates and cupolas were designed to withstand prolonged heavy bombardment (in fact, one withstood 24 hours of directed air attack¹⁴). Shape charges were designed to rapidly penetrate and destroy the entrenched defensive positions. So where is the new battlefield of the Digital Blitz...the civilian owned critical infrastructure.

The original 8 critical infrastructure of the United States as listed in Presidential Decision Directive 63 are

1. Water
2. Gas oil storage and delivery
3. Government operations
4. Electricity
5. Emergency services
6. Banking and finance
7. Telecommunications
8. Transportation

While it would be difficult to attack even half of the original 8 simultaneously, they do provide a good road map to smaller scale engagements. Furthermore, since they are owned by U.S. corporations on U.S. soil there are limits, as to the involvement of the United States military. Following McRaven's theory of Special Operations, we will narrow the scope of any one attack and keep the operation simple. This helps improve the chance of mission success. Also, keep in mind that a wounded target costs more than a destroyed one. So let's walk through a sample series of attacks.

Step 1 – Pick your target. For the purposes of this paper, we shall be attacking a major national retail chain that has stores in every town of any size as well as a significant on-line presence. The goal is sustainable impact on local economies specifically and the U.S. economy in general.

Step 2 – Pick your general timelines. Use weather as your friend. Attack the west during wild fire season, the south-east during hurricane, the north during winter and the middle during the hottest part of summer.

¹⁴ Spec Ops, pg. 56

Step 3 – Choose a random or variable attack schedule. Terrorism breed fear through its sheer randomness and violence of action. The Washington D.C. sniper attacks held the D.C. metro area in fear for 3 weeks in October of 2002. The randomness of the targets and the timeline along with a specific threat against children created a collective state of fear and altered many behavior patterns.

Step 4 – Choose your specific timelines. For physical attacks, choose times that will impact the most people. Rush hour is a great example. Anything that shuts down a major transportation artery will have long lasting and immediate impact. During the D.C. sniper attacks, a close friend was stuck on the D.C. beltway for hours while it was shut down to look for ‘the white van’.

Step 5 – Choose your target domains. In our attack against the national retailer, we’ll go after as many of the 8 domains as possible:

1. Water. Water is your friend. Hacking into water controllers to shut off water to the retailer’s corporate headquarters is a great way to send everyone home early. After all, if there is no water, you can’t flush toilets and that becomes a health hazard. This attack also works well against their data center too.

2. Gas oil storage and delivery – Class 1 data centers require diesel generator backup. If the tanks are above ground, destroy them.

3. Electricity – Deny power through traditional physical attacks as well as digital. Attacking power supplies to the stores at peak shopping hours or high temperatures is key.

4. Banking and finance – Odds are that the headquarters is well secured from digital attacks against their finances. The trick here is to go after the smaller banks and credit unions of the employees. Digitally siphoning off money, preventing deposits and phishing for employee data to log into their accounts are all effective methods of attack.

5. Telecommunication - Executives and employees all use cell phones. If they are using Bluetooth headsets, we can listen in and even record conversations; a valuable source of intelligence. Also, most of the stores will have satellite or land lines back to headquarters for a variety of purposes (inventory, payroll, etc.) Working to get into the data stream will allow for man in the middle attacks, denial of service and data theft/corruption.

6. Transportation – Trucks move merchandise, cars move people. There are a variety of ways to delay traffic flows from taking over street lights and variable messaging signs to traditional kinetic attacks against roads.

Step 6 – Begin swarming. Attacking two or more target domains simultaneously. The more you can attack at once, the better. With retail outlets all across the country, there are targets anywhere. Furthermore, to simplify support and maintenance, chances are that if an attack works well at one location, it will most likely work again at other locations due to similar or even identical infrastructure. To maximize damage and sustainability, include low resource commitment physical attacks. These include random pipe bombings, bomb scares and shootings.

For those that doubt the power of even just digital attacks; look to the recent case of Blue Security. In the spring of this year, Russian hackers attacked the anti-spam company of Blue Security. After a multi-day cyber-war, Blue Security decided to close its doors rather than risk an all-out slug match.¹⁵ It is possible to run a company off the internet using only digital attacks.

The combination of digital and physical attacks against multiple domains of a target is the full realization of a Digital Blitzkrieg. A new form of fighting that takes the best from low intensity operations and computer network attacks and uses them against civilian owned critical infrastructure. Since any single attack requires little resource commitment; the pulse of fire is sustainable over a long period of time. Likewise, any single attack requires few people. The missing piece is someone or thing coordinating the timing of the attacks which is easily accomplished through a variety of chat rooms and cell phones.

Counter Blitz - Civilian Operated Red Cells

Red Cells are in use by every branch of the military, DHS and even in civilian circles. Loosely defined, a Red Cell is a team of professionals hired to test security. In the National Strategy for Homeland Security there was a call for the creation of Red Cells.¹⁶ These cells would be different than any in use today in two key factors.

1. They would focused on combined cyber and physical attacks
2. They would be staffed by civilians and be responsible directly to the federal government

With the advent of technology convergence, it is impossible to separate the physical and digital worlds. Surveillance cameras pump their signals across IP data networks. Vonage is signing up customers for VOIP internet telephony services. Bluetooth technology is used in automobiles and GPS has replaced traditional navigation skills. While a combined cyber and physical attack is inherently more complex to prepare for, the payoff is extraordinary. Cascading and down stream effects are great. For example, imagine controlling the traffic lights of a major metro area to over-congest an area and then triggering a series of IEDs at rush hour. The resulting chaos would be catastrophic. To combat this, we need Red Cells to operate on U.S. soil to recon and plan combined attack scenarios.

Furthermore, the teams who operate must be civilian staffed and managed. Law enforcement is not prepared for this type of work, and the military would have legal hurdles that might prevent them from conducting offensive planning operations against U.S. citizens on private property. The benefit of this arrangement would be teams who would be assigned to work up scenarios for various geographic regions. The resulting scenarios would then be turned over to the owner/operators of the affected assets for countermeasures and mediation. Lastly, the same scenarios could be used as starting points for multi-jurisdictional training operations.

Conclusion

The digital Pearl Harbor must be put to rest. In the rapidly converging, ever changing technology landscape, a new analogy needs to be created; one that accurately reflects potential attacks. Unlike

¹⁵ <http://weblog.infoworld.com/techwatch/archives/006432.html>

¹⁶ National Strategy for Homeland Security, Office of Homeland Security, July 2002

some, this paper is not a prophecy, but an extrapolation of trends. Ultimately, I would hope that additional resources are spent creating at least one Red Cell to train for combined cyber and physical operations in a simultaneous battle space. The goal is not to predict the future, but to prepare for as many possible futures as we can.

THIS PAGE INTENTIONALLY BLANK