Published by Cyber Magazine, 01 July 2017,
http://magazine.milcyber.org/stories/knockoutbycyberstrikefightinglikeits1989

Knockout by Cyber Strike – Fighting Like It's 1989

By John Dobrydney

The "Pearl Harbor" metaphor for a successful cyber strike against the United States is an apt one and provides a vehicle for the discussion of initial post-strike reactions and actions, and for suggested policy improvements aimed at deterring crippling attacks. Cyber attacks capable of exploiting critical vulnerabilities, such as the United States government's and commercial sector's excessive operational dependence on interconnected computer networks are exceptionally problematic to deter or, if attacked, to determine an appropriate response strategy. Therefore, this paper proposes the following hypothetical: A presumed nation-state launched a cyber strike against the United States, which successfully destroyed its cyber and networking capabilities, thereby rolling back the nation's ability to wage war as if it were 1989.

The hypothetical calls for several assumptions. The adversary will attempt a non-attribution attack to obscure the strike initiator and reduce the probability of counterattack. Kinetic or non-kinetic retaliation will be extremely difficult if the United States cannot categorically state who launched the attack and, likewise, other nations will be reluctant to use or condone military force for the same reason. The adversary will also calculate on the attack causing maximum damage and yet still remain beneath the threshold for war. This is, in any event, a challenging response for the United States, as there is no precedent for war in response to a cyber attack.

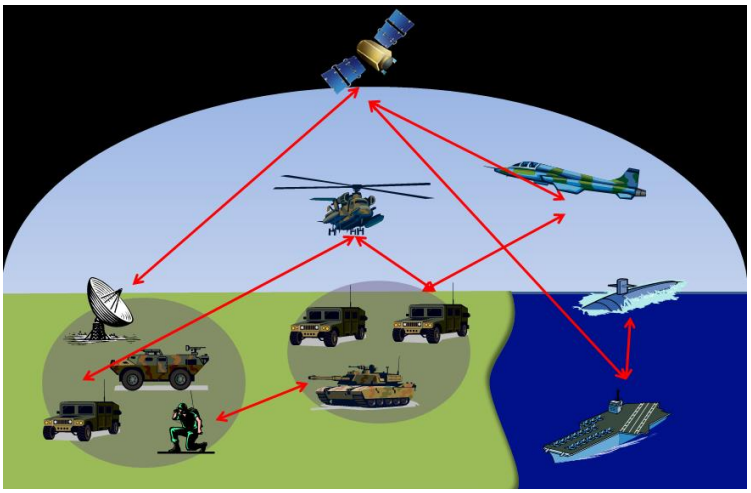
The United States will be most vulnerable to physical attack in the immediate chaos and confusion following a cyber strike. Since so much of the United States military's advantage is rooted in its highly networked command and control systems, a cyber strike will curtail its ability to conduct highly synchronized, well-planned operations or rely on technically advanced intelligence, surveillance, and reconnaissance (ISR) assets. Logistics planning and execution will rapidly lose synchronization, and commanders will quickly lose visibility on what resources they have, where they have them, and their material condition. One can assume that information stored in the "cloud" or on servers connected to the Internet will be corrupt until proven otherwise, or will not be available if the strike destroyed the storage point or the means to access it. Rarely is information stored in anything other than digital form, so information recall in support of operations and planning will be limited.

A paralyzing cyber strike will affect all elements of national power. Diplomatically, the United States will be in a weakened position because it failed to deter the cyber strike, and this position will only be exacerbated if the U.S. cannot attribute the attack or find a way to answer - either in

kind or via some other means. International solidarity may waver if there is no convincing cause to rally around.

Exceptionally strong leadership coupled with a messaging campaign signaling resolve and resilience will calm public reaction and focus the American people and the international community on solving the problems at hand. This will be challenging, as the normal modes of broadcast communication largely rely on the Internet. Use of newsprint, radio, town hall meetings, and other creative methods will have to suffice until system administrators restore Internet capabilities. Leaders from government and industry will need to cooperate on a way ahead considering both sectors rely on the same Internet for their critical services. This united front requires communication to and support from the public during the initial chaos, and follow-on Internet restoration and potential retribution against the attackers.

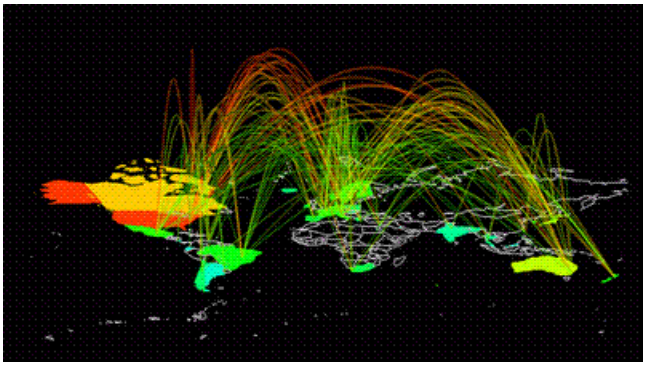
The United States would be militarily correct to assume that a kinetic attack would most likely follow a crippling cyber strike. Quickly raising defense conditions, possibly even considering a nuclear response if "the sleeping giant" deemed it necessary would signal that it is taking the cyber attack most seriously. Disasters such as Pearl Harbor in 1941 and 9/11 have shown that the American people "won't abandon any involvement" but will become "drawn in" and will want to see a tangible response.[1]



Military power relies heavily on cyber assets to provide it with its informational advantage over a wide range of adversaries and capabilities. Joint Publication 3-13 defines information superiority as "the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same."[2] David Albert highlights the competitiveness in information gathering: "Information Superiority in military operations is a state that is achieved when competitive advantage is derived from the ability to exploit a superior information position. In military operations this superior information position is, in part, gained from information operations that protect our ability to collect, process, and disseminate an uninterrupted flow of information while exploiting and/or denying an adversary's ability to do the same."[3] Destruction of the DoD Information Network in a cyber strike means that surface, sub-surface, land, air, and space sensors cannot communicate with each other to provide shared battlespace understanding. This lack of sensor information denies the United States the superior informational position necessary to exploit higher tempo operations or to negate an adversary's quantitative or even qualitative advantage. In short, an asymmetric cyber attack will level the information playing field by defeating its underlying physical network.

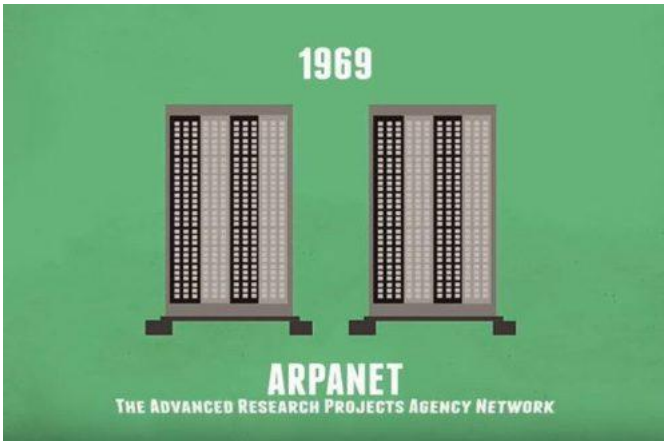
The economic disaster following such a strike will perhaps be the worst tangible effect, as it will cause a cascading global financial meltdown. Cyber attack targets will most likely include financial networks on Wall Street and institutions in other locations, as they are historically soft targets. They are an easy asymmetric attack that will greatly degrade US strategic strength and will instill fear in the populace via a very tangible plunging Dow Jones, decreasing 401(k) balances, and the pronouncements and reminders of a 24-hour media cycle. At best, the strike would cause a short-term lack of access to financial information, causing a recoverable 'hiccup' in the system. At worst, corrupted or lost data will lead to a data integrity problem and long-term financial market chaos. Firms will not know what they own, what they sold, or the value of what they hold on their books. To the extent that they can, investors will naturally sell off their stocks and bonds and subsequently tank the economy as fear and increasing uncertainty set in. Moreover, the dollar will lose value, possibly kicking off a cascading global financial collapse.

One "benefit" of the Internet's interconnectedness is that most nation states capable of a significant cyber strike on the United States have a stake in the interconnected global economy. Much like the global meltdown caused by the housing mortgage crash in 2007, the effects of a severe economic attack on the United States will cascade across the world and will, most likely, affect the nation that either launched or supported the cyber attack. However, as history has shown, the market will rebound and the United States' economic capacity is amazingly resilient. Congressional research following 9/11 showed that "the loss of lives and property on 9/11 was not large enough to have had a measurable effect on the productive capacity of the United States" and that "the overall economic impacts of the 9/11 attacks were even lower than initially estimated, indicating that the United States economy is more resilient in the face of disaster and intentional attack than commonly assumed."[4] It might be the case then that any country capable of launching a successful cyber strike against the United States will not be able to escape the metaphorical blast pattern and will only succeed in harming itself.



Joint Publication 1 both notes that cyberspace resides in the physical domain, and defines it as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures including the Internet, telecommunications, networks, computer systems, and embedded processors and controllers."[5] The physical domain supports information creation, storage, and transfer and is the physical network upon which the more familiar informational dimension — the World Wide Web — depends. Cyber is globally interconnected and ubiquitous; it supports the four elements of national power, all military warfighting domains, as well as virtually every global

commercial process. Therefore, an attack causing a cyber-service disruption will have a noticeable impact of varying degrees depending on the level of connectedness to the point of attack.



At its conception, the Internet's designers never considered how their creation might evolve to the phenomenon it is today. The small group of academics designed the ARPANET in 1969, in part, to provide an alternate communications path in the event that a nuclear attack disrupted primary communication routes. An ARPANET spinoff produced a rudimentary network that allowed academics to share their findings amongst participating United States universities. Membership was small, and a shared professional ethic disallowed foul play. As such, the system expanded without considering explicit security controls. Over the years, and with a desire to push new technology, the network expanded with the invention of the web browser to provide everyday users with access to the World Wide Web. Coupled with a virtually free telecommunications infrastructure left over from the dot-com boom and bust, the Internet grew virally throughout most industrialized countries. A "virtuous cycle" arose as faster computing power via the Internet led to more business productivity. In turn, greater productivity led to a desire for faster computing power, and so on.[6] Security was a minor concern in the design phase and soon became prohibitively expensive, and inhibited business operations when security managers added vulnerability mitigations as an afterthought.

Securing the Internet is largely a contest of measure and countermeasure. The inherent flaws and vulnerabilities in computer hardware, software, and in the users who operate and administer networks give both the initiative and the easier task to the offense. Any defense must be 100% foolproof, whereas an attacker needs only a single penetration to conduct whatever malicious activity he has planned. The defender requires skills in areas as diverse as preventing physical access to servers and routing hardware; preventing "social engineering" whereby an attacker deceives a user by phone, email, or in person to gain restricted network access; detecting malware injection via phishing scams; applying supply chain risk management, which seeks to secure the end-to-end supply chain; ensuring proper encryption use; ensuring new hardware and software versions do not introduce new vulnerabilities; and implementing cyber security controls properly so they do not introduce their own new vulnerabilities. Adding to a defender's problems is the fact that skilled attackers can hide their presence, which causes delay in attribution and response. Given enough time and resources (e.g., state sponsorship, education, and Internet provided information — ironically), the offensive has the upper hand.

Strategic actions and responses following a "Cyber Pearl Harbor" would be similar to the bold and unorthodox responses following the 1941 Pearl Harbor attack. In the aftermath following that attack, the United States found its strategy for countering and destroying Japanese aggression in the Pacific suddenly unfeasible, its means sidelined until repairs and new ships

came online, and its confidence severely shaken.[7] The attack sidelined the mobile fighting strength in the Pacific, its battleships, until the United States could shift to a wartime economy to reinforce remaining strength and support strategic ends. Fortunately, the remaining perceived American military strength deterred the Japanese from following through with a second strike on Pearl Harbor to destroy oil farms, shipyard facilities, and submarines. This gave the United States time to "catch breath, restore morale, and rebuild forces."[8] Driven by events, submarines and naval aviation took center stage following Chief of Naval Operations Admiral Stark's order six hours after the Pearl Harbor attack: "Execute unrestricted air and submarine warfare against Japan."[9]

The Pearl Harbor attack in 1941 and a Cyber Pearl Harbor attack in present times suggest several strategic parallels. Initial deterrence did not work, but for various reasons, Japan did not press its advantage. This point leads to another. Intelligence in late 1941 lost track of the Japanese carrier divisions and was unable to detect preparations and movements. It is far more foreseeable today that the United States would use its extensive ISR capability and the analytical capabilities within the intelligence community to detect preparations for an attack large enough to follow an initial cyber strike. For an adversary to wait and make preparations following a cyber strike would not only be a race against who can mobilize fast enough for decisive results but would also forfeit the element of surprise — one of the advantages afforded by a crippling cyber strike. No one, then or now, can match the United States' economic might. It would be prudent for an adversary to either launch a non-attributable cyber attack against the United States and then maintain normal operations or continue to cripple the United States with an electromagnetic pulse set off by nuclear weapons as a quick follow-up that needs little preparation time. Otherwise, the United States, as historically shown, will rapidly use overwhelming force.

The 1941 attack greatly changed the conduct of the Pacific war; likewise, a crippling cyber strike would change the conduct of a potential follow-on war.[10] War Plan Orange called for the battle line and supporting ships to steam west in defense of the Philippines and other United States territories in a climactic showdown with the Imperial Japanese Navy. December 7, 1941, obsoleted that line of thinking. Regardless, the new Commander-in-Chief of Pacific Fleet, Admiral Nimitz, a submariner by trade, had to use what he had at hand to defend Hawaii and the west coast of the continental United States, to conserve his fighting force for the long road to Tokyo, and to rebuild the destroyed fleet he inherited. Forced to center stage by events, the unscathed submarine force and naval aviation assumed starring roles in an initial strategic

defense — and later, an offense — of the Pacific. In today's context, a cyber strike will force Joint Force Commanders to use what they have at hand and will need the flexibility required to either revise or develop a new strategy that does not initially rely on information superiority until the United States can restore its networks and cyber capabilities. The technology, United States workforce, and economic potential would still exist, so it will be possible to rebuild the networks and capabilities over time. Small intranets firewalled from or not connected to the Internet during the cyber strike could still operate and provide rudimentary services and access to the network's information. In the interim, strategists may determine that the Internet and the current command and control model has been more of a hindrance to effective operations and by necessity *in extremis* may find another way to solve the problem, similar to aviation and submarines displacing battleships. For example, there has been much discussion on dispersion and swarming tactics that rely on decentralized decision making with only a generalized higher headquarters intent. Perhaps with today's advances in HF/VHF/UHF radio technology, units can adopt such methodology and still retain agility and flexibility, while higher headquarters make do with far less information and decision-making authority.

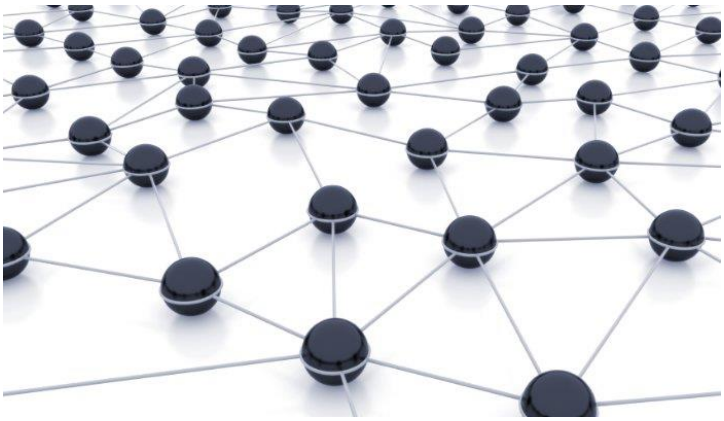
Given the United States' excessive operational dependence on its networks, a strategy to both deter a crippling cyber strike against the United States and to maintain a minimum level of operational capability, should such an attack occur, is called for. Deterrence must be real and tangible, and thought of as a "…psychological relationship; the goal is to shape an opponent's perceptions, expectations, and ultimately its decisions about launching an attack. Thus, deterrence requires an 'opponent' who is thinking, or might readily think of attacking. Ideally deterrence short-circuits that thinking…making it a deliberately contrived relationship with an opponent."[11] Further, "deterrence is not only used to prevent attacks and war via threats of harm. It is often used via attacks and war, that is, deterrence by doing harm."[12]

International informational and diplomatic signals that state that nations who engage in certain levels of cyber attacks will suffer tangible repercussions can be a powerful deterrent. Nuclear deterrence during the Cold War provides a precedent. Nations that used nuclear weapons could expect a nuclear response per the Mutual Assured Destruction policy. Capabilities assigned the mission of responding to a cyber strike must remain untouchable from the cyber domain, else the deterrent effect is lost and those forces be susceptible to the same cyber threats as any other network user.

The remaining problem is attribution. While greater emphasis and capabilities are required to determine an attack's point of origin, the United States should make it clear that the time delay common in determining attribution will not have an attached statute of limitations. Deterring a crippling nation-state cyber strike depends on adversaries absolutely knowing that a coalition of wide ranging resources will identify them, and that overwhelming harm will soon follow.

In case deterrence fails to stop a cyber strike, the United States must have a strategy of decentralization, resilience, and rapid healing. A good form of defense is to make the offense's capabilities irrelevant. In the case of the Internet in its current form, it will always have

exploitable vulnerabilities; therefore, networks will always be under varying levels of attack whether by state employed experienced hackers, amateur "script kiddies," or something in between. The goal should be to stay a few steps ahead of the attackers and maintain a level of survivability such that the command and control structure can still function, albeit in a restricted fashion. Decentralized network control is an effective method to rapidly respond to network attacks and prevent such attacks from propagating through the network. Users must know the role they need to play: "Disaster researchers have shown that victims are often themselves the first responders and that centralized, hierarchical, bureaucratic responses can hamper their ability to respond in the decentralized, self-organized manner that has often proved to be more effective."[13]



Resilience and rapid healing apply not only to the physical network itself but also to the infrastructure, agencies, and processes operating the network.[14] One characteristic of a well-designed communications network is that operators can expect a certain percentage of degradation and faults, and overall network operation will not suffer. If the primary route fails, then alternate routes are available during the time it takes to repair the primary. Well-designed networks require planning, constant attention to network operations, and well thought out policy that takes network failures into account. Failure recovery becomes a part of normal operations. Likewise, users who depend on communications networks for their operations must develop their own means of resiliency in case of network degradation, or even destruction following a cyber strike. Recalling the lessons of Pearl Harbor, resilience calls for an open mind, broad experience, and a willingness to innovate and take risks on unorthodox concepts. Designing a more resilient stock market, banking infrastructure, news media, government, and logistics organization that can operate on degraded or lack of Internet access will mitigate the effects of a potentially crippling cyber strike, and will ensure that organizations and users are better able to operate in a degraded environment. These social networks must have the same rapid healing characteristics as the physical network and must be part of normal operations. Increased resiliency in not only the physical network but also in the social networks, coupled with decentralized authority to take appropriate action with minimal communications capabilities, will reduce United States networking critical vulnerabilities, complement primary cyber deterrence means, and enable the United States to continue to execute its national security strategy with today's capabilities.[15]

About the Author

A Marine Communications Officer, Lieutenant Colonel John Dobrydney is an experienced cybersecurity and network operations planner. He recently served as the Commanding Officer of Marine Wing Communications Squadron – 18, the Executive Officer of 7th Communication Battalion, the Network Operations Officer for the III MEF G6, and served as the Enterprise Information Assurance Branch Head at Headquarters, Marine Corps C4 Directorate. He currently serves as the Cybersecurity Division Chief, Joint Staff J6. Lieutenant Colonel Dobrydney has a Masters of Security Studies from the Marine Corps War College and a Master of Science in IT Management from the Naval Postgraduate School.

End Notes

1. Sean Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History," *Mercatus Center at George Mason University*, 2011, http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

2. Alberts, David S, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare*, (Washington, DC: CCRP Press, 2003), 54.

3. Sean Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History," *Mercatus Center at George Mason University*, 2011, http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

4. Alberts, David S, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare*, (Washington, DC: CCRP Press, 2003), 54.

5. Joint Chiefs of Staff, Joint Publication 1, Washington, DC: DOD, 2009. P. I-7.

6. Carey, Davis and John E. Morris, *King of Capital*, (New York: Crown Business, 2012), 149.

7. Gordon Prange, *At Dawn We Slept*, (New York: Penguin Books, 1991), 582.

8. Ibid.

9. United States, ed., *How We Fight: Handbook for the Naval Warfighter* (Washington, D.C.: U.S. Government Printing Office, 2015).

10. Alan D. Zimm, *Attack on Pearl Harbor*, (Philadelphia: Casemate, 2011), 385.

11. National Research Council (U.S.) et al., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), http://site.ebrary.com/id/10425159.

12. Ibid.

13. Sean Lawson, "Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History," *Mercatus Center at George Mason University*, 2011, http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf.

14. Ibid.

15. Ibid.

Photo credits (in order of appearance): salon.com, TELEGRID, forbes.com, TruthHugger.com, History of Domain Names, navy.com, linkedin.com, LinkedIn