2018

The Cyber Pearl Harbor redux: helpful analogy or cyber hype?

Wirtz, James J.

Routledge, Taylor & Francis Group

James J. Wirtz (2018) The Cyber Pearl Harbor redux: helpful analogy or cyber hype?, Intelligence and National Security, 33:5, 771-773, DOI: 10.1080/02684527.2018.1460087
https://hdl.handle.net/10945/71678

INTELLIGENCE AND NATIONAL SECURITY, 2018
VOL. 33, NO. 5, 771–773
https://doi.org/10.1080/02684527.2018.1460087

Routledge
Taylor & Francis Group

ARTICLE

The Cyber Pearl Harbor redux: helpful analogy or cyber hype?

James J. Wirtz

ABSTRACT

This article defends the utility of employing the Pearl Harbor analogy to characterize contemporary cyber threats, especially threats facing the United States. It suggests that despite the fact that policy-makers are keenly aware of the nature of today's cyber threats, this knowledge does not necessarily protect them from falling victim to a strategically significant cyber surprise attack. The fact that elected officials and senior officers fall victim to strategic surprise attacks launched by known adversaries is the *problematique* that animates the study of intelligence failure. The article concludes with the observation that just because scholars and policy-makers can imagine a 'Cyber Pearl Harbor' does not guarantee that they can avoid a Cyber Pearl Harbor.

After reading James Boys' history of the origins of U.S. cyber security policy, it is hard to escape the conclusion that Al Gore might not have been the father of the Internet, but he sure had a ringside seat during America's initial foray into cyber security. Boys does an outstanding job of chronicling the William J. Clinton administration's efforts to protect the United States against cyber attack, efforts that were both farsighted and sophisticated at a time when issues of cyber crime, cyber war, and cyber terrorism were largely confined to the realm of futurists and real computer scientists. 'The Clinton Administration's Development and Implementation of Cybersecurity Strategy (1993–2001),' is an important contribution to the intelligence literature because it highlights how scholars and officials alike have long been attuned to the security risks created by the ongoing threat of cyber attack and how they have taken steps to mitigate that menace. Contemporary observers debate whether or not past and current efforts are containing cyber threats, especially given the lightening-fast pace of change prompted by the Information Revolution. Nevertheless, Boys convincingly demonstrates that senior U.S. policy-makers had cyber security on their minds before most people sent their first email.

What sets my pen to paper is that Boys uses the Cyber Pearl Harbor analogy in general, and my paper on that topic in particular, as a straw man to be knocked down by his history.[1] Boys asserts that using the Cyber Pearl Harbor analogy to characterize the cyber threat is misleading because policy-makers would not be surprised by a cyber attack given that it has been on their minds for over 30 years – note the Clinton administration's sophisticated cyber awareness evident by the early 1990s. In Boys' view, the United States might suffer a strategically significant cyber attack, but it is misleading to say that U.S. officials would be 'surprised' by that eventuality.

Admittedly, using the Pearl Harbor analogy to characterize contemporary cyber threats is controversial. Many believe, with good reason, that all this 'Pearl Harbor talk' might just be cyber hype spouted to fatten agency budgets or to line the pockets of executives hawking the latest computer security software.[2] Indeed, my motive for writing 'The Cyber Pearl Harbor' was to demonstrate that a cyber surprise

CONTACT James J. Wirtz ✉ jwirtz@nps.edu

attack could be integrated into a strategy to achieve some territorial, military or political objective. In my view, angst about a potential surprise cyber attack seemed detached from political or strategic reality, as if an opposing government's officials would one day decide to bring down the U.S. electric grid, banking system, or stock market 'because they can.'[3] By contrast, I believe that a Cyber Pearl Harbor is a real threat because a cyber surprise attack would provide a weaker opponent with an opportunity to negate U.S. deterrent strategy and present the United States with a relatively bloodless fait accompli and a painful military, diplomatic, or political dilemma. Specifically, U.S. policy-makers would have to learn to live with the new situation or engage in a kinetic campaign to return to the *status quo anti bellum*.[4]

What is odd about Boys' use of the Cyber Pearl Harbor analogy as a straw man, however, is his suggestion that those who recognize the general outlines of a threat can never be surprised by that threat. That assertion is simply not true. Surprise occurs despite the fact that victims have a deep awareness of the threat they face; this very phenomenon is the *problematique* addressed by the literature on intelligence failure and surprise attack. A few examples should suffice to make this point. Israeli officials were aware that Egypt and Syria were deeply hostile in the fall of 1973, yet they fell victim to a strategic surprise attack. Even clear signs of an impending threat cannot avert disaster. Joseph Stalin received scores of direct and indirect warnings of an impending Nazi invasion, but this did not prevent the Soviet Union from falling victim to a nearly existential strategic surprise attack.[5] Bill Clinton, upon first learning of the 9/11 attacks, blurted out 'Bin Laden did this' before he received official confirmation of who was responsible for hijacking those airliners. For that matter, Israeli officials or Red Army officers were not 'surprised' by who was doing the shooting as their territory was invaded. Nevertheless, the degree of situational awareness expressed by Clinton did not prevent the countries just listed from suffering a strategic surprise attack.

It is especially ironic that Boys chose this particular straw man for his foil. If Boys' assertion is correct – prior knowledge precludes surprise – then the Pearl Harbor analogy itself would not exist because American officials had ample evidence of the vulnerability of their fleet to Japanese attack prior to 7 December 1941. The scenario was the subject of games conducted by faculty and students at the U.S. Naval War College in the 1930s. Additionally, during Joint Army and Navy exercises undertaken in February 1932, Admiral Harry E. Yarnell approached Oahu from the north with the aircraft carriers Saratoga and Lexington. His mission was to attack U.S. forces on the island. He selected his approach based on the poor weather north of the Hawaiian Islands to mask his task force's movement and the day to attack, Sunday, to catch the defending forces in a vulnerable position after a Saturday night well spent in Honolulu. Yarnell reached a position 60 miles northeast of Oahu undetected. He then launched 152 planes, which simulated attacks against airfields, depots, headquarters, and ships at anchor.[6]

Yarnell's success might have been forgotten by the fall of 1941, but one event in particular should have made the threat of Japanese attack on Pearl Harbor salient to members of the Franklin Roosevelt administration, including the President himself. Senior U.S. Navy officers objected to the movement of the Fleet to Pearl Harbor for a variety of reasons, including its vulnerability to attack. In fact, they delivered a powerful protest under the signature of Admiral J.O. Richardson, Commander of the Pacific Fleet, to the President himself, stating 'The senior officers of the Navy do not have the trust and confidence in the civilian leadership of this country that is essential for a successful prosecution of a war in the Pacific.'[7] Richardson was relieved following the receipt of that message, but it is hard to believe that the issues that prompted that protest faded quickly from the minds of officials in the Roosevelt administration or senior officers. By December 1941, officials in Washington recognized that Japanese–American relations had reached a nadir;[8] nevertheless, Yarnell's escapade or Richardson's protest did little to highlight that deployment of the Fleet to Pearl Harbor was not a deterrent, but a weakness that the Japanese could not ignore.

Boys highlights that the Clinton administration was aware of the cyber threat facing the United States, possessing the foresight to suggest that the threat would increase as the Information Revolution gathered steam, to use an inappropriate metaphor. But to say that threat awareness itself forever inoculates future generations against a strategic surprise attack is not born out by history. In fact, Boys' narrative actually helps to fit the Pearl Harbor analogy more closely to our current situation. Like the Roosevelt administration, contemporary policy-makers should consider themselves forewarned: the United States faces the threat of a strategic surprise attack using cyber weapons and responsible people have been issuing warnings about this situation. Time will tell if such an attack actually occurs, or if the United States can defeat that attack pre-emptively or if defenses can mitigate the threat before it produces catastrophic results. Indeed, a successful defense would negate the applicability of the Pearl Harbor analogy to the contemporary cyber threat. Nevertheless, the fact that you can imagine a Cyber Pearl Harbor does not mean you can avoid a Cyber Pearl Harbor. Officers and officials alike have to be on the *qui vive*.

Rest assured, I am rooting for the home team; I hope that the scenario depicted in 'The Cyber Pearl Harbor' never materializes. To that end, I have developed some practical suggestions for avoiding a strategic surprise attack exploiting cyber.[9] Still, the history here, as highlighted by the Pearl Harbor analogy itself, is not particularly encouraging.

Notes

1. Wirtz, "The Cyber Pearl Harbor," 758–67.
2. Valeriano and Maness, *Cyber War versus Cyber Realities*.
3. For further development of this issue see my review of the Valeriano-Maness volume cited above, Wirtz, "Cyber War or Monkey Business?"
4. Wirtz, "The Cyber Pearl Harbor."
5. For a recent volume that demonstrates how policy-makers involved in the Israeli and Soviet cases were acutely aware of the threats they faced and still fell victim to a strategic surprise attack see Bar-Joseph and McDermott, *Intelligence Success and Failure*.
6. Fleming, "February 7, 1932 – A Date That Would Live In…Amnesia."
7. Baer, *One Hundred Years of Sea Power*, 151.
8. Sherman, "William Friedman and Pearl Harbor," 309–27.
9. Wirtz, "The Cyber Pearl Harbor."

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

James J. Wirtz is dean of the School of International Graduate Studies at the Naval Postgraduate School, Monterey, California. He is the author of *Understanding Intelligence Failure: Warning, response and deterrence* (Routledge, 2017). He is the former chair of the Intelligence Studies Section of the International Studies Association.

Bibliography

Baer, George W. *One Hundred Years of Sea Power: The U.S. Navy, 1890–1990*. Stanford, CA: Stanford University Press, 1994.

Bar-Joseph, Uri, and Rose McDermott. *Intelligence Success and Failure: The Human Factor*. New York: Oxford University Press, 2017.

Fleming, Thomas. "February 7, 1932 – A Date That Would Live In…Amnesia." *American Heritage* 52, no. 5 (July/August 2001). https://www.americanheritage.com/content/early-warning.

Sherman, David. "William Friedman and Pearl Harbor." *Intelligence and National Security* 33, no. 3 (2018): 309–327.

Valeriano, Brandon, and Ryan C. Maness. *Cyber War versus Cyber Realities*. Oxford: Oxford University Press, 2015.

Wirtz, James J. "Cyber War or Monkey Business?" *The International Journal of Intelligence and Counterintelligence* 31, no. 2 (2018): 415–419.

Wirtz, James J. "The Cyber Pearl Harbor." *Intelligence and National Security* 32, no. 6 (2017): 758–767.