Lessons Learned in World War Two Pacific Are Relevant to Today's Cyber Security Challenges

(Originally published in Defense Systems on June 26, 2012)

by Mike McConnell

Earlier this month, I had the pleasure of speaking at a commemoration in Hawaii of the 70th Anniversary of the allied victory at Midway — a critical turning point in the war in the Pacific and one that was largely made possible by the U.S.'s ability to break Japanese codes, thereby allowing Pacific Commander Admiral Nimitz to know where the enemy was — and where they were headed.

The Battle of Midway happened a long time ago, but not so long ago that I haven't had the pleasure of crossing paths with some of its key figures. My role, as a former Naval Intelligence officer and the nation's chief code breaker as the Director of the National Security Agency in the 90's, was to provide context and to introduce a real American hero and one of last surviving members of Admiral Nimitz's code-breaking team, Rear Admiral Max Showers. As a 22-year-old ensign, Admiral Showers was a hands-on participant in the successful code breaking and code group recovery effort that turned the war.

As he spoke with riveting clarity at the Midway commemoration, RADM Showers told listeners he was "absolutely certain, despite all the books and articles that have speculated otherwise, the US did not have the information and could not have prevented the successful Japanese attack on Pearl Harbor." While RADM Showers has always served as a role model and inspiration for dedicated public service to me, I have to differ with my respected, senior friend – and it's a disagreement that pertains not just to the past, but, more importantly, to the future.

The U.S. was successful in breaking the Japanese Imperial Naval code "after Pearl Harbor" because that is when we were forced to put the needed resources and talent on a problem of national significance. Had we started our code breaking efforts at the same level of commitment and intensity in the late 30's or even in 1940, we would have been successful in decrypted and translating information to provide Japanese intentions and the disposition of their forces well before Pearl Harbor.

Is Past Prologue?

Today, we find the nation in very much the same posture as 1941, albeit pre-December 7, 1941. The former CIA Director and present Secretary of Defense, Leon Panetta, has stated that our next catastrophic event is likely to be a "Cyber Pearl Harbor" It's hardly scaremongering. The nation is bombarded daily by nation-states with policies of cyber

economic espionage that are successful extracting terabits of sensitive, competitive information that drives the US business engine. Our strength has been our ability to invent and innovate and this information is being massively taken on a daily basis. Additionally, nation states are building thousands of cyber-attack tools intended for degradation and destruction in war or conflict. Sooner or later, some of these cyber-attack tools will get inadvertently released in the cyber global commons or intentionally sold to some terrorist group hoping to change the current world order to fit their view of the future.

We have the information and ability today to prevent a Cyber Pearl Harbor. The question is, will we take steps to avoid it, or will we wait for it to happen? The US Intelligence Community (USIC) recovers vast amounts of threat vector information that could be used to screen and protect the nation – in both the public and private sector. However, our current laws and policies do not allow the USIC to share the information in an effective way – their hands are tied, a dynamic that serves only our foes,. While there are as many as seven draft bills in Congress to address these issues, the arguments against are framed by concerns for privacy and civil liberties on one side and concerns about "regulating" industry on the other.

Public-Private Partnership: It's Achievable (and A Model Already Exists)

To protect the nation, we need robust and timely sharing of sensitive information between the government and the private sector in a "public-private" partnership.

Of course, nearly any time the prospect of public-private partnerships involving IT security are discussed, the concept is battered, equally, by two somewhat opposing camps — on one side, privacy advocates and, on the other, those who oppose any regulation of businesses.

I believe that the privacy concern can be addressed via legislation and regulation that clearly defines what would be illegal practices for the government to do, and the regulation concern could be addressed via opt-in-only mechanisms that encourage participation via a number of benefits, including more information, liability protections and the benefits of standards.

The more critical point is that there is an excellent model already in place for a public-private partnership, focusing, no less, on information sharing in the IT space, and its roots go back nearly 50 years.

The National Security Telecommunications Advisory Committee (NSTAC) facilitates information sharing between the public and private sectors related to threats to the operations of our national telecommunications infrastructure. Having evolved out of the National Communications System, which began in the JFK era, NSTAC works — for the

shared benefit of the public — and it works well. It's one example of a model for cooperation that could be harnessed to address today's growing cyber threats.

Beyond the example of NSTAC, there's a more fundamental truth at hand. Good security – whether cybersecurity or any other kind of security — requires *communications*, namely the controlled sharing of relevant information. If you don't have that – or deny the common sense that underpins it — you're only going to have a facsimile of security, not the real thing.

Now is the time for all sides to relax opposition to work together to frame and pass the needed legislation for effective cyber defense. Otherwise, like Pearl Harbor and 9-11, we will strongly react "after the fact" when damage has been inflicted. What a waste.

Mike McConnell is a former vice admiral in the United States Navy. During his naval career he served as director of the National Security Agency (NSA) from 1992-1996; serving first under President George H. W. Bush and later under President Clinton. As a civilian Mr. McConnell served as the Director of National Intelligence (DNI) for two years, a position of Cabinet rank, under Presidents George W. Bush and Barrack Obama. He is currently Vice Chairman at Booz Allen Hamilton.