Anticipating Future Cyberattacks on the High Seas

https://www.e-ir.info/2017/09/20/anticipating-future-cyberattacks-on-the-high-seas/

DAN G. COX AND BRUCE STANLEY, SEP 20 2017

There was a great deal of speculation and confusion surrounding recent naval mishaps involving US military ships in the Pacific Ocean. Initially, confusing reports by crews on both the container ships that crashed into the USS Fitzgerald and the USS McCain and the navy crews on these Aegis cruisers were uniform in their claims that no radar alert or alarm sounded before either crash. Speculation regarding a cyberattack conducted by a third-party state with advanced cyber capabilities, like those possessed by China and Russia, began to surface. However, the US Navy claims that there is no current evidence of a cyberattack in either case. Recent assertions by current and retired naval officers have gravitated around a lack of training and incompetence as being more likely causes for the four recent naval accidents in the Pacific theatre. Still, the US Navy is leaving no stone unturned and continues to simultaneously probe the human error and potential cyberattack angles as causes for the recent spate of crashes. This entry does not aim to engage in the debate over whether or not the naval accidents were cyberattacks or a series of naval mishaps. Instead, since at least one notable security expert, Csaba Krasznay, argues that ship navigational systems are very vulnerable to cyber-hacking, we are going to explore the strategic implications of a future cyberattack on US naval assets. In this way, we are going to explore a future scenario in order to anticipate some of the strategic challenges that it poses to policymakers and military planners.

In order to illustrate the strategic and operational implications of a future cyberattack on US Navy ships, we are going to borrow some of the facts from the current naval incidents and extrapolate these facts into a speculative near-future. We are going to focus on the McCain and Fitzgerald incidents since these two incidents involved strategically important Aegis cruisers. Aegis cruisers provide the most advanced missile defense system against short and medium range missiles. Therefore, they are integral in the Pacific theatre given the missile threat emanating from North Korea and the potential entanglement with China which possesses on of the most advanced missile threats against naval assets in the world.

In our future scenario, two Aegis cruisers are attacked by cyber-hijacked containers ships in the Pacific Ocean. The incidents occur only months apart from one another and twenty US seamen are killed in the incidents. However, unlike the current incidents, it becomes readily apparent that these incidents are not the result of error but, instead, are a result of cyber-hacking by a near-peer competitor state. Both incidents occurred in the early morning hours when both the container ships and US naval ships were running skeleton crews. In both cases, the ships began running parallel to one another and then the container ship turned around and eventually maneuvered itself so it was aimed to ram into the side of the Aegis cruiser. Both attacks nearly sank their targeted Aegis cruiser and both resulted in the loss of life on each ship. Despite not sinking, both cruisers suffered significant damage and had to be taken back to a U. S. port for repairs that will last for years, effectively removing them from the theatre for the foreseeable future.

The first crash between a civilian container ship was odd enough to spark a high-level investigation which resulted in no concrete evidence of malfeasance. Even though both the crew on duty on both the Aegis cruiser and the container ship reported no radar signal or alarms prior to the crash, the investigative crew concluded that these crews were misleading the investigators in order to cover their own incompetence. Eventually, the Captain of the Aegis cruiser, the executive officer, and the lieutenant on duty the night of the crash were relieved of duty.

After the second crash, US cyber-analysts discovered a discrepancy in the time the second container ship and second Aegis cruiser collided. The container ship reported the crash occurred at 3am while the US Aegis cruiser crew report the crash occurred at 4am. Suspecting that a third party infiltrated the navigational system of the container ship but were unable to reset the clock to local time, the computer analysts dig further into the programming code for the navigational system. As they dug deeper into the computer code controlling the container ship, they found clear evidence of cyber-hacking. Unfortunately, they could not find evidence linking a single nation-state to the attack.

At this point the strategic ramifications of the attacks become evident. The nation conducting the attacks has attacked U.S. military targets, disabled both of these targets, and killed U.S. servicemen and women. It is clearly an act of war *but* it may not or will not necessarily be interpreted as such. We will now delve into the reasons why this is so. There are several sacrifices and risks that policymakers and military leaders have to consider. If the incident is made public, the American public will demand retribution, perhaps even in the form of war, because twenty sailors were killed in the attack. However, if the attack is not made public, then military leaders will be forced to end the careers of possibly able military officers in order to give the impression to the enemy and the public that the cause of poor seamanship.

What the near-peer competitor has done in this hypothetical future scenario is ratchet upward the gray zone of conflict. The enemy has seized the initiative and put the American political and military leadership on the horns of a dilemma where a clear attack on U. S. military assets may best be kept in the shadows. The strategic options are limited and carry grave risks. The United States can ignore the attacks and play dumb while attempting to figure out how the attacks were perpetrated. The United States could levy economic sanctions but this is unlikely as the attack would then be public knowledge and the American public is unlikely to be satisfied with sanctions as retaliation. The United States could figure out how the attacks were conducted and by whom and begin a similar campaign against the belligerent. This is an extremely dangerous outcome as now low-level warfare is being conducted between two major military powers in a new, expanded gray zone. The United States could go to war with this near-peer competitor. The obvious risk here is that war between such great military powers could eventually include the use of nuclear weapons and, even if it does not, it will surely result in millions of dead soldiers and civilians.

Current events which many are portraying as poor seamanship allow us a window into a possible future. This prospect is either possible now using current computer hacking technology or it will be possible in the near future. The results of this scenario are sobering and the strategic conundrums this scenario poses are great. Assuming away both cyberattacks and an expansion of the gray zone is a sure recipe for experiencing fundamental strategic surprise.

About the author:

Dan G. Cox is an Associate Professor of Political Science at the School of Advanced Military Studies, Fort Leavenworth, Kansas. He has three published books: *Terrorism, Instability and Democracy in Asia and Africa*, *Population-Centric Counterinsurgency: A False Idol*, and *Stability Economics: The Economic Foundations of Security in Post-Conflict Environments*. He also regularly published in peer-reviewed journals and magazines. He has served as part of the NATO Partnership for Peace program helping to improve the professional military education system for the Republic of Armenia. He currently serves as the Reviews Editor for Special Operations Journal and on the Board of Executives for the Special Operations Research Association.

Bruce Stanley is an associate professor at the School of Advanced Military Studies with a PhD from Kansas State University in Security Studies. He is also the author of the book Outsourcing Security, Private Military Contractors and US Foreign Policy. He is a retired Infantry Officer with over 24 years of service in the Army.