Why Are Our Ships Crashing? Competence, Overload, and Cyber Considerations

By Chris Demchak, Keith Patton & Sam J. Tangredi
August 25, 2017

U.S. Navy photo by MC2 Joshua Fulton

This article originally appeared at CIMSEC. These are exclusively the personal views of the authors do not necessarily reflect the views of the U.S. Naval War College or the Department of Defense.

Security researchers do not believe in coincidences. In the past few weeks, a very rare event – a U. Navy destroyer colliding fatally with a huge commercial vessel – happened twice in a short period of These incidents followed a collision involving a cruiser off Korea and the grounding of a minesweepe the Philippines, and have now resulted in the relief of a senior Seventh Fleet admiral. Surface warfa officers (SWOs) look to weather, sensors, watchstanders, training requirements, leadership and regulations (COLREGS) as possible contributing factors to the collisions.

Cyber security scholars, in contrast, first look to the underlying complex technologies trusted by the to determine the proper course of action. With the advancements in navigational technology, compu aided decision making and digital connectivity, it is human nature that seafarers become more depe on electronic aids for navigation and trust the data the systems provide. While the U.S. Navy empha

commercial vessels over 500 GRT (gross registered tons). As of 2016, 87 percent of merchant shipp
uses satellite navigation and 90 percent of the world's trade is carried by sea. Nonetheless, ship cap
can turn it off and travel without identifying themselves (at least until detected by other means). U.S.
vessels do not routinely transmit AIS but each bridge monitors the AIS of ships around them in addit
the military and civilian radar systems and the eyes of the sailors.

In quiet or tense times, the bridge watch and the Combat Information Center (CIC) teams of naval warships must synthesize this information and make sound decisions to avoid putting the ship into extremis. This is a continuous, round-the-clock requirement and a tough task for even the most skille

In this photo released by Japan's 3rd Regional Coast Guard Headquarters, the damage of Philippine-registered container ship ACX C is seen in the waters off Izu Peninsula, southwest of Tokyo, on June 17, 2017 after it had collided with the USS Fitzgerald. (Japan's 3r Regional Coast Guard Headquarters/AP)

In contrast, merchant ships such as the *Alnic* MC, a chemical tanker (which hit *JOHN S. McCAIN*) h tiny crews with great reliance on autopilot. Depending on the circumstances, possibly only three peo would be on the watch as the ship's commercial navigation autonomously follows the route that the captain set initially. One of the indications that the *ACX Crystal*, the cargo vessel colliding with the U *FITZGERALD*, was on autopilot was its behavior after the collision. Having been temporarily bumpe its course by the collision, it corrected and resumed steaming on the original course for about 15 mi before stopping and turning to return to the collision location. While nothing is yet published about w was happening on either bridge in the June *FITZGERALD* collision, one can surmise that it took 15 minutes for the small crew to realize what had happened, to wrest control back of the behemoth, an it around.

Possible "Normal" Explanations

Flawed human decision-making

U.S. Navy warships maintain teams of watchstanders in order to mitigate the effects of a flawed dec being made by any one individual. Ultimately, one individual makes the final decision on what action take in an emergency—the Officer of the Deck (OOD) if the Commanding Officer is not available—b recommendations from the others are assumed to help in identifying flaws in precipitous decisions b they are actually made.

In contrast, in merchant ships with only two or three deck watch standers, there is less of a possibilit flawed decision-making is identified before incorrect actions are taken. These actions can also be influenced by unrelated disorienting activities. Alcohol is not permitted on U.S. warships, abuse of dr at any time is not countenanced, and U.S. naval personnel are subjected to random urinalysis as a means of enforcement. On a merchant ship these policies vary from owner to owner, and inebriation decision-making under-the-influence has contributed to many past collisions.

Common tragedy from fatigue in an inherently dangerous environment

Collisions at sea happen. U.S. warships have collided with other warships, including aircraft carriers with civilian vessels. USS *FRANK EVANS* was cut in half and sunk in 1969 when it turned the wrong and crossed the bow of an Australian aircraft carrier. In 2012 the USS *PORTER*, a destroyer of the s class as the *FITZGERALD* and *MCCAIN*, was transiting the Strait of Hormuz. The *PORTER* maneuv to port (left) to attempt to get around contacts ahead of it, passing the bow of one freighter astern an then being hit by a supertanker it had not seen because it was screened behind the first freighter. M the previous collisions involved a loss of situational awareness by an at-least-partly fatigued crew. It hard to avoid such conditions in an inherently dangerous, around-the-clock operating environment.

Mechanical Failure

There has been no report of a problem with the *FITZGERALD*prior to her collision. The Navy, howev has acknowledged the *MCCAIN* suffered a steering casualty prior to the collision. While backup stee exists in the form of manual controls in aft steering or using differential propulsion to twist the ship in absence of rudder control, such control methods are not as efficient as the normal controls. Addition there would be a brief delay in switching control unexpectedly or transmitting orders to aft steering. I normal conditions, this would not be serious. In a busy shipping lane, with the least hesitation due to shock at the unexpected requirement, the brief delay could be catastrophic.

Quality of training for ship handling by young Surface Warfare Officers (SWOs)

One can look at the U.S. Navy Institute *Proceedings* (the premier independent naval journal) and oth literature to see signs these incidents may be symptoms of a larger issue involving the training of wa standers. In March 2017, LT Brendan Cordial had a *Proceedings* article entitled "Too Many SWOs p Ship" that questioned both the quality and quantity of the ship handling experience that surface warf officers (SWOs) received during their first tours. Later in a SWO's career track, the focus of new department heads (DH) is tactical and technical knowledge of the ship's weapons systems and ship combat capabilities, not necessarily basic ship handling. Ship handling skill are assumed. But such s can atrophy while these officers are deployed on land or elsewhere, and individual ships have uniqu handling characteristics that must be learned anew.

In January 2017, CAPT John Cordle (ret.) wrote an article for Proceedings titled "We Can Prevent S Mishaps" and called into question the modern SWO culture. Peacetime accident investigations rarel produce dramatic new lessons. They simply highlight past lessons. Errors in judgment, lapses in coordination, task saturation, fatigue, a small error cascading into a tragedy. Those who have stood watch on the bridge or in the CIC read them, and frequently think, "There, but for the grace of God, g However, unlike in the aviation community, near misses and accidents that almost happened were n publicly dissected and disseminated to other commands. Officers have always known how easy it is

publicly dissected and disseminated to other commands. Officers have always known how easy it is relieved for minor mishaps, but they do not have the community discussion of all those that nearly happened to learn vicariously from the experiences.

Pace of forward operations – especially for the MCCAIN after the FITZGERALD event

Both destroyers are homeported in Yokosuka, Japan, the headquarters of the U.S. Seventh Fleet. W only the line of duty investigation has been released for the FITZGERALD collision, one can assume the officers and crew of the McCAIN would have heard some of the inside details from their squadro mate. Logically the CO of McCAIN would be doubly focused on the safe operation of his ship as he approached the highly congested traffic separation scheme (TSS) in the straits of Malacca and appr to Singapore harbor. But the loss of one of only seven similar and critical ships in a highly contested environment would almost certainly increased the tempo and demands on the MCCAIN as it attemp move into the Singapore harbor just before sunrise.

In this case, tempo should have been accommodated adequately. While technology is a key compor of U.S. warships, it is only one of many tools. Lookouts scan the horizon and report contacts to the b and CIC watch teams. The officer of the deck (OOD) uses their professional skills and seaman's eye judge the situation. If in doubt, they can, and should, call the Captain. Indeed, close contacts are rec to be reported to the Captain. The bridge and CIC have redundant feeds to display contacts detecte radar, sonar, or AIS. The computer can perform target motion analysis, but crews are still trained to manually calculate closest points of approach and recommend courses to avoid contacts via maneu boards (MOBOARDs). This is done both on the bridge and in CIC so even if one watch misses some critical, the other can catch it. When ships enter densely trafficked areas, additional specially qualifie watchstanders are called up to augment the standard watch teams. Yet, it is possible that—under th theory of "normal" accidents—somewhere in this multiply redundant sensor system, misread or mish information led to the human equivalent of the "telephone game" and the wrong choice was dictated helm.

But along with the "normal" explanations, the possibility of cyber or other intentional distortion of criti data does remain a possibility.

Cyber Misleads and Mis-function

If one argues that neither the Navy nor commercial crews were inebriated or otherwise neglectful, ac that the weather and visibility were good for the time of day with crew in less stressful routine sailing postures, finds serendipitous mechanical failure of severe navigational significance on both ships dif to accept as merely normal accidents, and questions if tempo distraction alone could explain both ev then – as Sherlock would say – the impossible could be possible. It is worth laying out using unclass knowledge how cyber intrusions could have been used to cause warships to have collisions. This is say the collisions could not have multiple sources. But for the purposes of this thought experiment, however, this section will focus on cyber explanations.

Cyber affects outcomes because it is now a near universal substrate to all key societal and shipboar functions. Either cyber errors mislead humans, or its digitized operations malfunction in process, act effect, or both while buried inside the complex systems. To make this point, one of the two major cla of cyber assaults – the distributed denial of service (DDOS) – works by using what the computer wa do anyway – answer queries – and simply massively overloads it into paralysis. It has been shown i number of experiments that large mechanical systems integrated with electronics can be remotely m to overload, overheat, or vibrate erratically into breakdown by hackers or embedded malware. In sev reports, the *McCAIN*may have suffered failures in both its main steering system (highly digitized) an backup systems (more mechanical). Less information has been released on the earlier collision betv the *FITZGERALD* and the *ACX Crystal* cargo ship so steering issues there cannot be known at this

However that the two collisions involved large commercial ships with similar crews and technologies

However, that the two collisions involved large commercial ships with similar crews and technologies that two U.S. Navy vessels were sister ships close in age and technologies suggests commonalities could be more easily exploited by adversaries using cyber means rather than humans. In particular, commonly shared logistics or non-weapon systems such as navigation are more likely to have vulnerabilities in their life cycles or embedded, routinized processes that are less sought by – or discernible to – the standard security reviews.

In a complex socio-technical-economic system like that involved in both circumstances, the one-off r event is likely the normal accident – i.e., the *FITZGERALD* incident. But too many common element present in the *McCAIN* event to suggest a second, simply rogue outcome. Hence, it is necessary to explore the three possible avenues by which the navigation could have been hacked without it being obvious to the U.S. Navy commander or crew in advance.

First, external signals (GPS, AIS) can be spoofed to feed both navigation systems with erroneous information for any number of reasons including adversary experimentation. Second, the civilian cor management systems on the civilian or military bridge (or both) could be hacked in ways either serendipitously or remotely engineered to feed erroneous data. Third, insider-enabled hacks of one both of the destroyer's combat systems could have occurred in the shared home port of Yokosuka to enable distortion of sensors or responses under a range of possible circumstances.

Spoofing GPS inputs to navigation

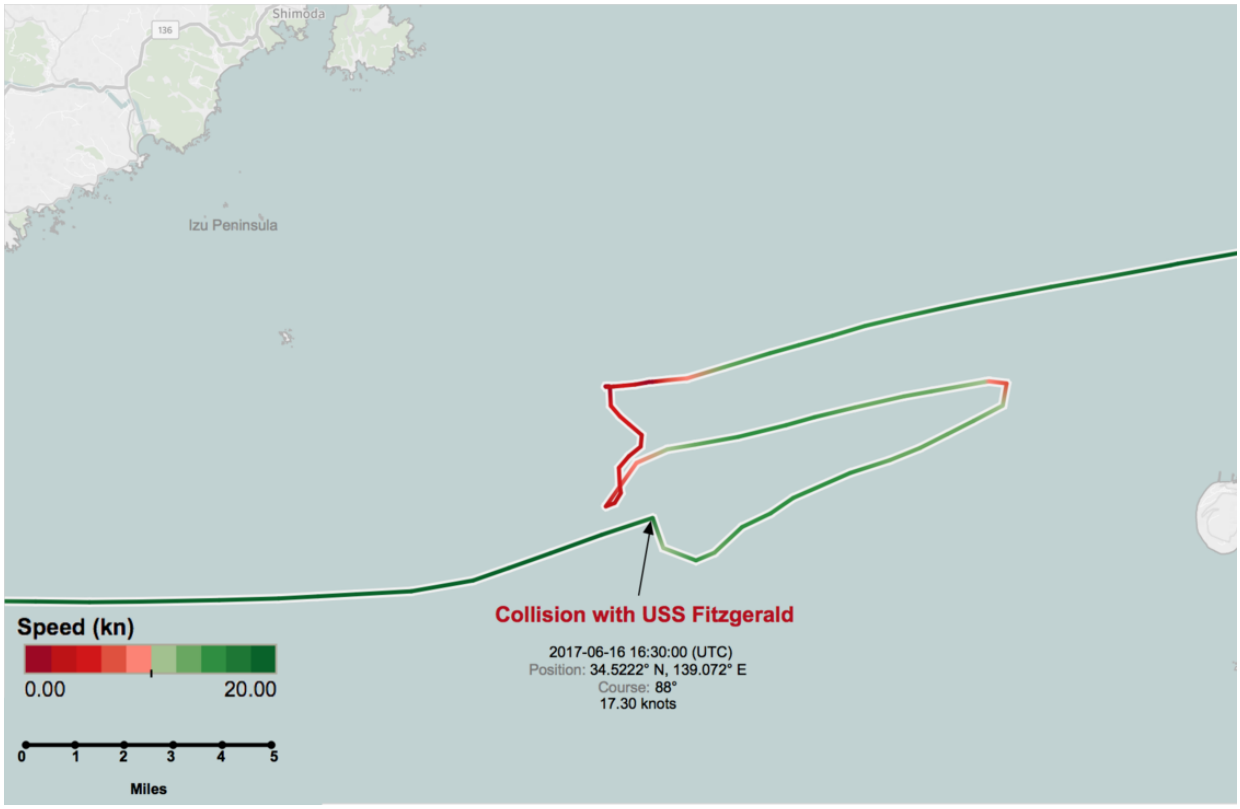
It does not take much technical expertise to spoof or distort GPS signals because the GPS system it sensitive to disruptions. The 2016 removal of one old satellite from service caused a 13.7 microseco timing error that occurred across half of the 30-odd GPS satellites, causing failures and faults aroun world in various industries. Anything that can be coded can be corrupted, even inadvertently. Anythi critical globally which does not have enforced, routine, and rigorous external validity tests, defenses corrective actions, however, is even more likely to attract the hacks from both state and nonstate act

Major national adversaries today have indicated interest in having the capability to arrange GPS distortions. With their already large domestic units of state-sponsored hackers, the Chinese, Russia and North Koreans have already sought such capabilities as protections against the accuracy of larg U.S. missile guidance systems. Hacking GPS has been reported for some years, and while some ef to harden the system have been pursued, spoofing mechanisms located on land in tight transit area even on other complicit or compromised vessels could mislead the autopilot. The website Maritime Executive reported mass GPS spoofing in June 2017 in the Black Sea, impacting a score of civilian vessels and putatively emanating from Russian sources most likely on land nearby.

However, it does not have to be a matter of state decision to go to war to have this kind of meddling key navigation systems, especially if land or many other vessels are nearby. In a cybered conflict wo state-sponsored or freelance hackers would be interested in trying to see what happens just becaus can. Not quite a perfect murder because of the external sources of data, however, the spoofed or sp data would provide misleading locations in real time to autopilot software. Vessels and their bridge w operate normally in their steering functions with bad data. They go aground or collide. So might airpl And the distorted signals could then stop, allowing normal GPS signals to resume and indicate that something went wrong in navigation choices but not in time to stop the collision or with the attributio trace necessary to know by whose hand.

In these two cases, the DDG *FITZGERALD* looks like it failed to give way to the *ACX Crystal* which appears by the tracking data to have been on autopilot. If the *ACX Crystal*'s navigation was operatin false data, and the equivalent civilian system on the U.S. ship was as well, then the watch team of th *FITZGERALD*would have had at least two other sources conflicting with the spoofed information – th military systems and the eyes of the sailors on watch. For the moment assume no deliberate hack o military systems, its radars are correctly functioning, and the alert sailors have 20-20 vision, then the watch team of the *FITZGERALD* clearly miscalculated by believing the civilian system. Or, the overla

relying on GPS is so profound that the military system was also fooled and the human eyes overrule
that case, the *FITZGERALD* watch team trusted the civilian system over other inputs.



AIS data map of course of container ship MV ACX Crystal around the time of collision with USS Fitzgerald near Japan on June 16, 2(
(Wikimedia Commons/marinetraffic.com)

In the *McCAIN* case, if one assumes all the same conditions, the Navy ship had the right of way and
oil tanker plowed into it. Presumably the tanker autopilot – if it was on as one could reasonably assu
was coded to stop, divert, warn, and otherwise sound the alarm if it sees another ship in its path.
Presumably, its code also embeds the right of way rules in the autopilot's decision-making. A convin
GPS spoof could, of course, persuade the autopilot navigation that it is not where it was, thereby see
more time and space between it and the Navy ship.

Hacking civilian navigation radars shared by all vessels

According to experts, commercial navigation systems are remarkably easy to hack quite apart from
spoofing. The cyber security of these bridge systems against deliberate manipulation has long been
neglected. In the same unenforced vein as the voluntary identification requirement of AIS, the globa
maritime shipping industry has relied on requirements by maritime insurance companies and specifi
regulations to control individual shipping firms' choices in vessels technologies (and level of complia
Myriad reports in recent years discuss the increasing sophistication of sea pirates in hacking comme
shipping systems to locate ships, cherry pick what cargo to go acquire, show up, take it, and vanish

shipping systems to locate ships, cherry pick what cargo to go acquire, show up, take it, and vanish
before anything can be done. That is more efficient than the old brute force taking of random ships f
ransom.

In addition, shipping systems tend to be older and receive less maintenance – including time-critical
patches – more likely to be scheduled with infrequent overall ship maintenance in port. In the recent
“Wannacry” ransom-ware global event, the major shipping company Maersk – profoundly and exper
hit – reported its key systems used WIN XP unpatched and unsupported by Microsoft. Hacking grou
also targeting ports and their systems as well.

If systems are compromised, hacks could have opened back doors to external controllers or at least
inputs when the commercial ship crossed into locations close enough to land or adversary-comprom
surface or submerged vessels. Then the misleading inputs could be more closely controlled to be pr
when U.S. vessels have been observed to be traveling nearby or are in a particular position. Navy v
may not transmit AIS, but they are detectable on radar as ships. A radar contact without an AIS iden
could be a trigger for the malware to at least become interested in the unidentified vessel, perhaps
sending pre-arranged signals to remote controllers to track and then wait for instructions or updates
autopilot would then act on the inputs unaware of the distortion.

An interesting aspect of corrupting code is that exchanging data across commercial systems alone c
provide a path for corrupted code to attempt to install itself on both ends of the data exchange. Stux
traveled through printer connections to systems otherwise not on any internet-enabled networks. If t
civilian navigation systems are proprietary – and that is likely the case on commercial ships – then it
likely that the U.S. vessels’ bridges also have ‘hardened’ COTS civilian systems whose internal softv
and hardware are proprietary. That means a hack successful on the commercial side could open an
opportunity to hack a similar or targeted civilian system that happens to be found on a U.S. Navy ve
Furthermore, it is possible the two systems share vulnerabilities and/or have exchanges that are not
visible to external observers.

Navy IT security on vessels might also regard the civilian proprietary systems as less a threat becau
they are not connected to internal military systems. They presumably are standalone and considered
merely an additional navigation input along more trusted and hardened military systems. The comm
systems are (ironically) also less likely to be closely scrutinized internally, because that would mean
U.S. Navy is violating contractual rules regarding proprietary commercial equipment. Outside of war
which such holds are likely to be ignored in crises – there is little incentive to violate those proprietar
rules.

One can conceive of a Navy bridge hosting a commercial navigation system that at some point alon
journey is compromised with nothing to indicate that compromise or the triggering of the software no
interwoven with the legitimate firmware inside the equipment. By happenstance, the Navy vessel co
in to the vicinity of an appropriately compromised large commercial vessel. At that point, the adversa
hackers might receive a message from the commercial vessel to indicate the contact and have the c
to distort the navigation inputs to help the commercial vessel’s autopilot plow into the warship.

Of course the adversary is helped if the Navy equipment is also hacked and, perhaps, the vessel los
digitized steering right before the impact.

Hacking U.S. Navy military navigation systems

Remotely accessing and then changing the triggers and sensors of military systems – if possible – w
be very hard given the Navy’s efforts in recent years. That possibility is tough to evaluate because th
open source knowledge regarding such systems is likely to be third party information on proprietary
subordinate systems at least five or six years old – or much more. Both major U.S. adversaries in As
North Korea and China – already show propensities for long-term cyber campaigns to remotely gain
access and infiltrate or exfiltrate data over time from all military systems, including shipborne naviga

access and infiltrate or exfiltrate data over time from all military systems, including shipborne naviga
We deem this less likely simply because this is where the cyber security focus of the Navy and DOD
already is.

However, the history of poorly coded embedded systems, lightweight or incompetent maintenance, a
deep cyber security insensitivity of third party IT capital goods corporations is appalling across a my
industry supply chains, even without the national security implications well-known today. While
commercial vessels could be hacked remotely, a more likely avenue for entry in Navy systems would
through these corrupted supply chains of third parties, shoddily constructed software, or compromise
contractors creating or maintaining the ship's navigation and related systems. Using insiders would b
especially easier than remotely hacking inside when the vessels were in a trusted harbor nestled ins
long-term ally such as Japan. Using insiders to access the systems during routine activities would be
likely to be detected quickly, especially if the effects would not be triggered or felt until particular
circumstances far from port and underway.

An especially oblivious contractor engaged in using specialized and proprietary software to patch, ch
or upgrade equipment could inadvertently use compromised testing or patching tools to compromise
vessel's equipment. For example, a Russian engineer carrying in a compromised USB stick was
reportedly the originating source of the Stuxnet malware in Iran – whether he was witting or unwitting
unknown. The actions would have been the same. Furthermore, Navy systems are built by contracto
with clearances of course, but the systems would have deeply buried and often proprietary inner
operating code. Corrupted lines of code could rest inactive for some time, or be installed in the last
minute, to lie dormant during most of the deployment until triggered. None would visibly display any
corruption until the programmed conditions or triggers are present.

In hacked systems, triggers are really hard to discern in advance. In part, the skill of the adversary d
obscures them, but also the objectives of adversaries can vary from the classic "act on command of
national superiors," to "see how far we can get and how," to pure whimsy. With no real personal cost
likely for any of these motives, the game is defined by the skill, patience, and will of the adversary,
especially when proprietary commercial code is involved. While it is safer in terms of attribution for
hackers to have more automatic triggers such as those used in the Stuxnet software, the action trigg
do not have to be automatic. In navigation systems, data is exchanged constantly. Conceivably there
be a call out and return buried in massive flows of data.

Without extensive AI and rather advanced systems management, how massive data flows are monit
can vary widely. While it is more and more common to secure a system's outgoing as well as incomi
communication, a multitude of systems that are not particularly dated have been shown to allow rath
subtle communications to go on for some time without any event or external revelation. One can ima
code calling home or acting autonomously when triggered by something as mundane as a sensor no
the presence of a large commercial cargo ship within X nautical miles, moving in Y direction, and
responding to encrypted queries from its own navigation system. Highly skilled botnet masters are a
detect anomalies across thousands of infected computers and, in a pinch, de-install huge botnets in
minutes. It is not difficult to imagine something buried in these otherwise secured systems, especiall
the adversary is willing to wait and see when it would be useful. For North Korea, the latest ratchetin
tensions between the Hermit dictatorship and the U.S. could easily provide a reason.

Hacking seems more of a possibility when considering how both destroyers failed to navigate under
circumstances that were, to most accounts, not that challenging. It is possible that the first such eve
the *FITZGERALD* collision – was a rogue event, the kind of complex system surprise that routinely b
rarely emerges. What is less likely is that a similar ship in broadly similar circumstances shortly there
proceeds to have a similar event. Exquisitely suspicious are the reports of the failure of the steering
system and possibly its backups on *McCAIN*, though not on the *FITZGERALD*. That effect is not spo
GPS or hacked civilian systems, and it would take much more reach of the malware to achieve. In
keeping with the presumption here that a successful insider hack occurred on both ships and the ma
was waiting for a trigger, the lack of steering failure (at least no reports of it) on the *FITZGERALD* co
also mean the malware or external controller was smart enough to know collision did not need addit
failures to ensure damage. The ship was already in the wrong place having failed to cede right of wa

Holding fire like that would be desired and expresses sophistication. Typical technique in cybered cc
is deception in tools; adversaries do not burn their embedded hacks unless necessary. Once shown
cyber mis-function becomes unusable again against an alert and skilled opponent such as the U.S.

Furthermore, the Aegis destroyers – of which both Navy vessels are – suffer from a rather massive
knowledge asymmetry with a major adversary. At some point in the early to mid 2000s, the Chinese
the entire design of the AEGIS systems on which the Navy spent billions across contractors and
subcontractors. While built to roughly the same specifications as a class of ships, each vessel reflec
upgrades and systemic changes of its particular era, with the older 1990s ships like the *FITZGERAL*
McCAIN having more patches and bolt-ons than the newer versions of the ship. Fundamental ship
elements are hardwired into the vessel and hard to upgrade, while more modular and likely proprieta
modern systems are plugged in and pulled out as time goes on. The adversary who stole those
comprehensive plans would know more about the older AEGIS ships than they would about the ship
completed after the plans were stolen and newer systems used in the installs. Anyone who has ever
faced the daunting prospect of rewiring a large house knows by ugly personal experience that the ne
wiring is forced to work around the existing layout and limitations. Ships are even more rigid and, qu
often, the more critical the system, the less flexibly it can be changed.

Thus, vulnerabilities built into the highly complex earlier AEGIS systems would be both known to the
thieves after some years of study and perhaps covert testing on other nations' AEGIS systems, and
very hard to definitively fix by the Navy itself, especially if the service is not looking for the vulnerabil
Unnerving, but not inconceivable, is the failure of the digitized steering system on the *McCAIN* – if it
happened. Exceptionally telling, however, is the presumably near-simultaneously loss of backup sys
If the steering and contact management systems were compromised, steering could be made to fail
the right time to force a collision. A good insider would be needed to ensure both, but only an advers
with considerable engineering design knowledge could reliably hazard a successful guess about hov
disable the more likely mechanical backup systems. The adversary to whom the original AEGIS thef
attributed – China – is known to be very patient before using the material it has acquired.

Both Civilian and Military Systems

Why not hacks on both systems? Commercial vessels are easier and could be left in place for some
pending being used and, in the meantime, slowly embedding Trojans via maintenance in port or thirc
party access to remove and replace proprietary boxes or upgrades in software. Preparation of the cy
battlefield occurs – as does the 'battle' – in peacetime well before anything or anyone is blown up. C
and North Korea have thousands of personnel on the offensive and value extraction cyber payroll.
Careers could easily be made by such coups of installing such software as potential tools and have
still in place ready to be used months or years later.

Furthermore, Westerners are routinely afflicted with the rationality disease of believing that all action
especially if adversaries are suspected – must be intentionally strategic and logically justifiable.
Otherwise, why would the adversary bother? There is also a tendency to underestimate the
comprehensive approach of most adversaries working against the U.S. Silence does not mean
compliance or concession on the part of adversaries, especially not China or North Korea. Installing
access points or triggers on all possible systems within one's grasp is a basic long-term campaign
strategy. Even now, when a major hack of a large corporation or agency is found, it has often been i
place for years.

Motives for the Collisions

Timing may be serendipitous, but at least one adversary – North Korea – has already sunk a naval v
of a U.S. ally, South Korea, with no public punishment. Certainly, North Korea has been loudly threa
the U.S. in the region and has cyber assets capable of what has been described above. However, o
difficulty in determining culpability is that, while China is an ally of North Korea, neither will readily sh
information so valuable as the AEGIS design plans or even what each other may have hacked. One

readily ascribe eagerness to hurt the U.S. physically to North Korea, but attributing the same motiva
China at this point is problematic.

There are other possibilities, however. Both nations – like most nations – are led by individuals with
technical comprehension. In particular and most unfortunately, in a world of ubiquitous cybered conf
where 'just because one can' or 'just to see what could happen' operates equally well as a motivatio
adversary states with a large army of hackers and technically ignorant superiors could easily have th
own cyber wizards working in ways their superiors can neither discern nor realistically curtail. In this
the *McCAIN* case (and possible *FITZGERALD*), these over eager technically skilled subordinates cc
have gotten quite lucky.

Why a DDG that happens to be sailing around Japan? Why one near Singapore? Why now? Well,
not" is as good a reason, especially if the U.S. Navy publically fires the ships' leadership and declare
incidents over. In that case there are no consequences for adversaries. Perhaps the *FITZGERALD* v
the rogue event, but—following that—the N.K. leaders then asked their wizards to take out another a
signaling or retribution for recent US "insults." That motivation has some persuasive aspects: no pub
apparent risks; a nifty experiment to see what can be done if needed in larger scale; and the public
turmoil alone puts North Korea with a smug secret while the U.S. twists trying to figure it out. Cyber
offensive capabilities in the hands of technically incompetent leaders have serious implications for m
and, critically, inadvertent outcomes that are strategically more comprehensive and potentially
destabilizing than ever intended.

Implications for the Navy

If it is leadership that failed in both cases, the Navy has a long history of responding and clearing ou
incompetence. If it is cyber that undercut that leadership and killed sailors, the Navy has an uphill ba
definitively establish all the avenues by which it could have and did occur, including fully recognizing
multiple sources of such deliberately induced failure. The literature on complex large-scale system
surprise and resilience offers means of preventing multisource failures in socio-technical systems.
However, these means may not be compatible with current Naval thought and organization. The liter
recommends parsing larger systems into self-sufficient and varying wholes that are embedded with
redundancy in knowledge (not replication or standardization), slack in time (ability to buffer from inpu
routinely), and constant trial and error learning. Trial and error learning is particularly hard because i
routinely involves violations of current practices.

The current organization of the U.S. military seems incompatible with the concept of easily decompo
units engaging and disengaging as needed in collective sense-making. Neither can it accept constan
systems adjustments, pre-coordinated but dynamically flexed rapid mitigation and innovation, and w
systems discovery trial and error learning. The truth is that in the cybered world, nothing can be trus
it is not reliably verified by multiple, independent, and alternative sources of expertise. USS *FITZGE*
did not discern its error and correct fast enough to avoid being in the wrong place at the wrong time.
McCAIN may have trusted its right of way entitlement too long, or made a traffic avoidance maneuve
suffered a steering casualty at the worst possible moment. Or perhaps both ships encountered some
unexpected: a commercial ship operating on corrupted code. In the future, we should expect that an
merchant ship controlled by digital information technology can be hacked.

This is a new idea for the Navy, that merchant shipping can be used as proxies for adversary intentio
With over 50,000 of such large vessels sailing around and next to U.S. ships all over the world, the
adversary's tools of coercion would be both effective and effectively obscured to visual or other indic
of malice. The world of cybered conflict is deeply riven with deception in tools and opaqueness in or
and now it is clearly on the seas as well. Even if the Navy rules that both incidents were simply bad
shiphandling, adversaries have already seen the great impact that can be had by making relatively f
Navy ships collide with big, dumb, large commercial vessels. Even if cyber did not play the deciding
in these events, there is every reason to assume it will in the future. Just because they can try, they

Dr. Chris C. Demchak is the Rear Admiral Grace Murray Hopper Professor of Cyber Security and Di of the Center for Cyber Conflict Studies, Strategic and Operational Research Department, Center fo Naval Warfare Studies, U.S. Naval War College.

Commander Keith "Powder" Patton, USN, is a naval aviator and the former Deputy Director of the Strategic and Operational Research Department, Center for Naval Warfare Studies, U.S. Naval War College.

Dr. Sam J. Tangredi is professor of national, naval and maritime strategy and director of the Institute Future Warfare Studies, Strategic and Operational Research Department, Center for Naval Warfare Studies, U.S. Naval War College.

verification of this data by visual and traditional navigation means, the reality is the social acceptanc
the validity of electronic data is a feature of modern culture. The U.S. Navy, with an average age in t
early 20s for sea-going sailors, is not immune from this effect. But what if the data is invalid or, as ar
extreme possibility, subject to outside manipulation?

In directing a pause for all warship crews (not currently conducting vital missions) during whicl conduct assessments and additional training, th Chief of Naval Operations – Admiral John Richa – was asked whether the Navy was considering intrusion as a possible cause. The CNO respon that concerning cyberattack or intrusion, "the re will consider all possibilities."

The truth could be that only mundane factors contributed to the accident, but as an intellectua thought experiment, what follows are explanatio following the logic of open-source information. T first set of explanations will focus on the human loop to argue that the fundamental cause is like human miscalculation rather than intentional distortion of data. The second explanation will focus on the criticality of accurate data provided to hu or their technologies. The pattern suggests a lack of 'normalness' as the 'normal accidents' of comp systems deeply integrated with cyber technologies – in frequency, locations, and effects. In the case the destroyers, a credible case—based on analysis of land-based systems–could be made for a witt unwitting insider introduction of malicious software into critical military navigation and steering syste The conclusion will offer motivations for timing and targets, and some recommendations for the futu

Similarities in the Scenarios

There are similarities in recent collisions. Both happened in darkness or semi-darkness. Both happe shipping lanes in which literally hundreds of major ships pass per day, to say nothing of smaller ship fishing vessels. Crew manning of both vessels approach 300 sailors, with approximately one-eighth crew on watch involved in controlling/steering, navigating, as lookouts, and operating propulsion machinery when the ship is at its lowest states of alertness, known as peacetime steaming. It is logi that both ships were at peacetime steaming at the time since they were not conducting military exer In contrast, when USS *JOHN S. McCAIN* conducted a freedom of navigation operation (FONOP) in vicinity of the artificial islands China has created to buttress its territorial claims to the South China S August 9, her crew was likely at high alert.

In looking for possible explanations, we have downloaded and examined readily available open-sou data concerning the two recent collisions, including identified locations of the incidents, vessel characteristics, crew manning, weather, proximity to land, automatic identification system (AIS) ship tracks, and shipping density data. We have consulted with naval experts on ship handling and on the of Japan and Strait of Malacca.

Collision avoidance on Navy vessels can be roughly cast into four elements, three technical and one human. On the bridge, the watch standers have (1) the AIS system which relies on tracking ships th broadcast their identities, (2) the military radar systems linked into the ships combat systems, (3)the civilian radar and contact management systems, and (4) the eyes of sailors standing watch on looko normally posted port, starboard, and aft on the vessel. All these systems are complementary and overlapping, but not exactly delivering the same information.

The AIS system – in which merchant vessels transmit their identities and location data – is an open voluntary system relying on GPS. In principle, keeping the AIS on is required for the 50 thousand plu