Cybersecurity's Role in Maritime Operations
International Seapower Symposium
September 23, 2016
James A. Lewis, Center for Strategic and International Studies

I would like to thank Admiral Richardson and the Navy for the opportunity to speak at this symposium. These remarks will provide an overview of the nature of cyber operations and attack, their implications for naval operations, and their strategic context.

Cyber operations provide new ways to coerce or defeat your opponents. Unfortunately, it also provides them with the same opportunities to defeat you. We should expect cyber-attack to form part of any future conflict. Cyber operations change the strategic landscape, as well as the nature of combat, much as the development of air power did in the last century. Then, navies discovered that ships operating without air cover or air superiority struggled to survive. Ships operating without cyber superiority will face a similar struggle.

This sound like hyperbole, and cyberwarfare may be one of the most misused terms in the strategic lexicon. Its nature is usually exaggerated, but more importantly, misrepresented. Cyberspace means the collection of computers, software and connections that link people, economies and countries. In cyberspace, Beijing is as close as the building across the street. Cyberspace is formed by networked devices and computers, powerful tools that we depend upon. That dependency will grow as everything from refrigerators to jet engines become cyber devices. The future is a more connected, more computer-dependent world. Computers and networks provide both superior capability and increased vulnerability. This has changed warfare. Computers are at the core of how modern militaries fight, and a military that doesn't use them may as well ride horses into battle.

Cyberattack create a new operational space for military action. For navies, the effect of cyberwarfare is to change the requirements for control of the sea, for creating maritime superiority, and for protecting commerce. It can incapacitate opponent decision-making and degrade or destroy equipment. While cyberattacks can produce effects similar to kinetic weapons, their intangible effects are equally important. An emphasis on kinetic effect can obscure important operational distinctions in the use of cyber techniques. There is an informational aspect involving the manipulation of data and decision-making. Complex cyber attacks would target ISR assets to create surprise and confusion. Cyberattack can shape the battlespace, enhance surprise, and create new fields for maneuver. Thanks to cyber operations, the opening stages of future conflict will involve even more confusion than we are used to seeing.

The nature of maneuver and engagement is different in this domain, since we are operating under a different set of physical and logical constraints. While proximity, distance and range remain important for actions that use electromagnetic signals, they are not significant constraint for operations on fixed networks, where traffic travels at the speed of light. This "domain" combines the electromagnet spectrum, information, and the internet's physical infrastructure. These create the space you will operate in, your targets, and the tools you will use to attack them. No one should be comfortable in the notion that one side or the other currently dominates the

electro-magnetic environment or that they do not face risk in cyberspace. Cyberattack will be part of any conflict with a competent adversary, and the first steps in a clash or conflict may take place in cyberspace.

Cyber operations change the requirements for effective tactics and operations. Submariners are used to maneuvering in an environment where they cannot see, but cyber warfare requires all operators to have a similar capability to conceptualize maneuver and effect, and to visualize not only kinetic action but intangible effects. Cyber operations are not fairy dust, some magical solution that can be sprinkled over military problems to make them go away, but they have reached the point of technical and operational maturity that makes them a valuable addition to the naval arsenal in both peacetime and conflict. Many commanders can have a general sense of their dependence on network and cyber capabilities, but they do not systematically review how their plans might be affected by cyber-attack. A review of what are assumed to be unique or short-lived cyberattacks does not provides a realistic assessments of the effect of a concerted attack and the risk this poses for operational success.

Cyber attack in not a weapon of mass destruction (WMD). It is possible to envision scenarios where a cyber-attack could achieve mass effect, by disabling large national networks, but this is not their most likely use. Such strategic-level attacks, particularly against an opponent homeland, bring greatly increased risk of conflict escalation and may not produce immediate military value. It could be possible to achieve mass effect form a cyberattack, but runs the risk of politically unacceptable collateral damage and only limited military benefit. Actions at the tactical and operations level are more likely. So far, state have used cyber operations in ways that are consistent with their doctrines and national strategies, but we have seen experimentation by opponents to test and to push the boundaries of conflict, linked to what some call hybrid warfare.

The Nature of Cyber Attack

We can assess cyber conflict by looking at known incidents. These incidents fall into three categories: coercive actions, disruptive actions and destructive actions. If we use conventional measurements of weapons effectiveness, the cyber "weapon" provides precision capabilities and has long range and high speed, but effect and consequences can vary in both duration and damage.

Calling cyberattack a weapon is an easy shorthand, but it is not the most precise best term to describe cyber operations. It may be better to think of cyberattack as an "exploit" rather than a "weapon," a combination of tactics, technology and teamwork to penetrate opponent systems and disrupt or destroy them. Known incidents suggest that the most damaging cyberattack have a high degree of precision. The trend in weapons development for the last several decades has been away from broad, indiscriminate effects and towards greater precision. In this, we can think of cyberattacks as a kind of digital precision guided munition (PGM). Precision weapons provide economy of force and greater predictability of effect.

All computer systems are vulnerable to attack. Modern weapons depend on software, digital data, and networking for optimal performance, and there is always a vulnerability in software –

no one can write millions of lines of code and not make a mistake, or more likely many mistakes. Air gapping doesn't work and static defenses are easily circumvented.

A major attack can take months to prepare, probing the target network and developing code tailored to damage, disrupt or destroy. Attacks have several stages: reconnaissance to identify the target's vulnerabilities, developing the attack software, breaking in, delivering the software "payload," and then "triggering" it – all without being detected. The capability to launch the most damaging cyberattacks, those that cause physical damage, are limited to only a few countries, but this will change as many other countries are developing these skills and disruptive software is widely available in cyber black markets.

This means that for now, cyber terrorism is a misnomer if by that term you mean groups like ISIS or Al Qaeda launching damaging cyberattacks. So far, they have not done so and there is no evidence that they have or are acquiring these capabilities. Every year for the last decade, there have been predictions that terrorist groups would turn to cyberattack. The law of averages suggests that eventually this may be right, but for now cyber conflict falls outside the capabilities of our opponents in the counterinsurgency efforts that have dominated military activity for the last fifteen years. Cyberattack is a tool reserved for states.

What would an opponent seek to do once they can access to your networks and devices? Clausewitz wrote of the fog of war, the uncertainty and doubt that slowed commander's decision-making. Cyberattack expands the fog of war. Ships and supplies can be misrouted. Sensor data can be manipulated or obscured. Communications can be disrupted or blocked. And in the best circumstances, opponents can be misled into firing on themselves. Cyber operations introduce uncertainty into the minds of opposing commanders, places the defender in an uncertain and reactive posture, and provides the attacker with the initiative.

Weapons and sensors are vulnerable. Your platform, weapon or sensor is running computer programs with thousands or millions of lines of code. A hacker gains surreptitious access to amend this code to introduce errors, or malicious commands to cause a crash or failure. Propulsion and navigations systems, port infrastructure, weapons sensors and communications are all good targets for compromise and cyber disruption. A cyber attack may produce obvious damage, but a sophisticated attacker would avoid a noticeable failure and instead but interfere with performance just enough to degrade it.

One example was a flight of F-22s deploying to Japan from Hawaii. When they crossed the international dateline, all their computers crashed – navigation, communications, sensors. Fortunately, the planes did not also crash, but they had to be guided back by a tanker aircraft. This was the result of a programming error but an opponent could intentionally introduce a similar error to produce a similar effect. Another early example involved the cruiser Yorktown, where computer glitches caused the propulsion system to fail, leaving the ship powerless. It had to be towed back to port. A third example involved the grounding of French naval aircraft whose computers were infected by a virus that had implanted itself on the navy's internal networks. All of these effects could be duplicated by hackers.

Leading cyber powers have undertaken operations to gain access to weapons systems software,

to understand their operational limits, perhaps to copy them, and to provide the possibility to interfere with their operations in combat. Press reports say that more than two dozen major U.S. systems have been hacked, including aircraft, drones, air and missile defense systems, and the littoral combat ship. Remember that cyber operations are a two-way street, and what has been done to the U.S also may have been done to others.

Tampering with opponent weapons and sensors is an important goal for militaries. Being able to access and corrupt that weapons software prior or during battle could significantly degrade performance. Illicit access to the software could take place during production, or when the weapon is temporarily connected to a network. In the field, radars provide a useful entry point, even if the radar is not attached to the internet. Radars receive a signal, process it and then pass it through a dedicated network to another system, operator, or weapon. A signal transmitted to a radar receiver could introduce malicious code or data that could degrade sensors, weapons, or command systems.

Cyber operations will merge electronic and cyber warfare techniques to gain entry and then to disrupt. Military systems offer different possibilities for the delivery of malicious software than are found in civilian cyberattacks. A missile, UAV, or projectile could create electromagnetic effect to introduce malicious software onto a target network. It is alleged that Israel used such methods against Syrian air defenses in an attack on a Syrian nuclear facility, and it is possible that advanced versions would interrupt sensor readings, disrupt links between sensors and weapons, and perhaps allow attackers to control opponent systems, or at least know what they are seeing. Cyberwarfare at sea will blend electronic warfare and its exploitation of opponent signals with cyberattack and the disruption of opponent software programs and computer systems to produce damage and effect that go far beyond conventional EW.

The machinery that propels and guides ships is vulnerable to attack. Industrial control systems, known as ICS, are special purpose computing devices used in a range of industrial applications, including ship engines, electrical generation equipment, pipelines and other equipment. As small computers they have little capability for self-defense and when they are networks, which is usual the case, they are of course subject to interference. A 2007 video of a test at Idaho National Labs shows how a malicious command remotely introduced into the ICS software controlling a room-sized electrical generator cause it to self-destruct. More recent examples include an attack on a German blast furnace, where the operators lost control, the attack on a Ukrainian electrical power facility, and the Stuxnet incident – in Stuxnet by the way, the target devices were air gapped and carefully monitored, to no avail.

In conflicts involving advanced powers, we should expect to see cyber-attack combined with electronic warfare, antisatellite attacks, informational campaigns and other unconventional tactics and weapons. We should not expect opponents to play by our rules or stay in the lanes we have laid out for ourselves. Opponent intent will be to degrade the American "informational advantage," to degrade communications and ISR assets and capabilities in order to hamper decision-making and operations.

Cyberattacks on naval networks could be combined with attacks on space assets. An opponent could attempt to disable satellite assets that support naval operations through a cyberattack on the

satellite control (or the satellite itself), in addition to any jamming or kinetic attack. Cyber, jamming and kinetic attack against space assets have been tested by several nations and other countries are developing a more limited set of anti-satellite operations that rely on cyberattack to degrade space services (such as navigation or communications).

Anti-satellite attacks considerably increase political risk in any conflict, but if they can be done covertly, this risk is greatly reduced. The reaction of the international community to overt space warfare would be uniformly negative, particularly if any kind of kinetic anti-satellite weapon is used, but the same is not true for electromagnetic or cyber-attacks on space assets, and some of our opponents, who have very different degrees of risk tolerance, may judge the political risk of kinetic attacks on space assets to be acceptable. The temptation, particularly in engagements between major powers, will be to use the full spectrum of EW, anti-space and cyberattacks to degrade informational advantage and inject confusion before turning to kinetic attack.

Cyberattacks are designed to exploit a particular configuration and set of vulnerabilities. Once the attack has been used, a defender can close vulnerabilities. This may limit the useful life of and exploit, creating what some call "single use" attacks. It also creates incentives for an attacker to strike early, since the opportunity for follow-on use may be limited. The greatest benefit of cyber-attack could come in the opening phase of conflict and increased cyber operations may be a warning of impeding attack.

"Single use" assumes that opponents will react and take defensive action – this is not always true in the civilian world, where known vulnerabilities can persist for months or years. Additionally, the software that runs industrial control systems or other hardware can be difficult to defend since these systems can be hard to patch or modify. In these circumstance, far from being single use, cyber exploits can be modified and reused. Attackers, however, do not know if they will have other opportunities and the least risk approach is to strike first. The tempo and duration of conflict also affects the constraints of single use. In a short, intense conflict, early single use may be best.

Some nations are concerned about developing "offensive' cyber capabilities, but a purely defensive approach guarantees always being in second place, always being reactive, condemned to always making the second move and always being surprised. The worry that acquiring offensive capabilities will "militarize" cyberspace is naive. Military cyber operations are entering their third decade. More importantly, many of your likely opponents already have offensive cyber capabilities, have trained and equipped forces to use them, and created doctrine for cyber operations. A good defense requires a knowledge of offensive capabilities. If it is politically more acceptable to call the full range of cyber capabilities "active defense," do so, but follow the example of NATO, which, without saying the words "offensive cyber operations," recognizes "cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea."

One of the unfortunate things about technological change in warfare is that a failure to keep up devalues your previous investment in equipment. If you don't adopt cyber operations, you are migrating your navies from operating ships to operating targets. This is a decision for political leaders, but the investment burden is softened if you consider that building cyber capabilities

means evolving your current EW and ISR investments into a new and expanded configuration that includes cyber operations. Creating cyber capabilities also requires creating a workforce pipeline to produce cyber operators and a career ladder for those operators – an early American mistake was to make the cyber operations specialty less attractive than other specialties. Note that all of these challenges are easier to meet if done in partnership with allies and friends.

Cyber Espionage

The skills required to penetrate a network are often the same whether intent is espionage or attack. The goal in espionage is not to attack but to exfiltrate information. Penetration of networks allows for the exfiltration of data on plans, capabilities and intentions. This is nothing new, but some opponents already have significant insight into your equipment, training, and doctrine, and perhaps into your warfighting plans as well.

Cyber espionage often relies on trickery and human frailty. A public example is the 2008 Russian penetration of SIPRNet. No damage was done, but the Russians were able to get in and the U.S. found it difficult to get them out. This would have provided immense advantage in conflict. The technique used, now widely known, was to throw an infected thumb drive in a parking lot. Someone picks it up, a normal human reaction, and plugs it into their office computer to see what's on it. The malware is then downloaded. This old trick and its variants work well for penetrating classified or air gapped networks

Another technique, called phishing, uses fraudulent email. The email has an infected attachment, and with the right title, many people will open it. One that works well in the corporate world is an email with an attachment entitled "next year's bonuses" – irresistible. Or websites can be contaminated so that anyone who visit them is infected. Sailors get social media messages from beautiful maidens saying they want to be friends. There is no end to human ingenuity in bypassing your defenses. So a good starting assumption for cyber operations is that you cannot secure your perimeter and must plan to operate in a degraded network and informational environment.

Coercion and Covert Cyber Operations

Information is not a weapon, contrary to what some of our Russian-speaking friends may say, but it can be used to coerce, threaten and manipulate. For example, Russia's 2014 Military Doctrine calls for "exerting simultaneous pressure on the enemy throughout the enemy's territory in the global information space…on land and sea." What is called "pre-conflict opinion shaping" will be part of any future conflict – you saw this recently in a somewhat clumsy fashion with the Russian announcement of Ukrainian attempts to assassinate a separatist leader, an effort to draw attention from their own military buildup. In the long term, these propaganda efforts may not work, but in the short term, they can complicate politics and morale.

"Pure" cyberwar," what we could call keyboard versus keyboard" or "geek versus geek"—is unlikely. Cyberattacks are fast, cheap, and moderately destructive, but no one would plan to fight using only cyber weapons. The goal in conflict is to blend them with other capabilities and weapons to achieve dominance. The goal in peacetime is to use cyber operations to obtain

advantage without leading to escalation in a response.

There is implicit agreement among nations that the kind of cyberattacks we saw used against Estonia in 2007 or by Iran against major American banks – called denial of service attacks – do not qualify as the use of force. Similarly, there is general agreement that attacks like Stuxnet or against the Ukrainian electrical facility, where there was physical damage, do qualify as the use of force. How to respond to the use of force is, of course, a political decision, but nations are beginning to define the political contours of cyber conflict.

Most cyber incident fall, however, in a grey area, not quite the use of force and intended to disrupt rather than destroy. The attack on the oil giant Aramco is an example of this. Aramco had the data on 30,000 hard drives permanently erased. Oil production was not affected but company operations were in disarray. The source of the attack was Iran, and the software may have been derived in part from black market tools. Opponents will exploit these grey areas in peacetime – think little green men – to make it more difficult to deter or respond to their actions. Cyber operations lend themselves to these new, "post-deterrence" strategies for conflict.

The Strategic Context for Cyber Operations

We have reached the end of a twenty-five-year period of strategic stability and relative peace among major powers. Stability means there is no incentive for a country to seek change through force or coercion. This is not the case for international relations today. We must recast our assumptions about strategy to recognize that we are entering a period of conflict. This will not be a new "Cold War" - the world is too interconnected for that, nor will it be World War Three - even without nuclear weapons, major combat operations against an advanced opponent are too expensive to be sustained for a prolonged period. Conflict between states will take new forms and in these uncharted waters the risk of miscalculation will only increase.

The future of war, at least among major powers, is that they will try to avoid direct conflict. Wars between big, heavily armed states are expensive and risky, particularly if they involve nuclear weapons. Big countries will not renounce war – Russia, the U.S. and China use force or the threat of force all the time – but they will try to avoid open warfare with each other. If big countries do stumble into war, cyberattacks will be a part of the fighting, but cyber operations are not waiting for the outbreak of armed conflict.

Cyber operations are a new way to exercise the fundamentals of national power, including force or the threat to use force. They are ideal for the new strategic environment. How countries will use cyber techniques is determined by their larger interests, by their existing strategies, experience, and institutions, and by their tolerance for risk. opponents will exploit the grey areas in international law and practice to do damage without triggering armed conflict.

The benefit of cyber operations, as with other elements of hybrid warfare, is that coercive force can be applied while minimizing the risk of violent response. This has implications for deterrence, for offshore operations and for the use of coercive acts. Deterrence will become harder and impossible in some conflictual situations, and we will see increased use of coercive acts that fall below the existing threshold for the use of force or armed attack.

There is of course, the temptation of covert action, a temptation to which many nations have yielded in cyberspace. To the extent an opponent believes they can take a cyber action and not be identified or observed, they will be tempted to engage. Attribution of cyber operations remains a problem, and since the foundation of international law and the right of self-defense requires identification of the attacker, the covertness of cyber operations offers the possibility of circumventing the rule the international community has developed to manage and limit conflict.

The status of international negotiations on cybersecurity remains slow and limited, far outpaced by the development of offensive techniques. There has been agreement on initial confidence building measures ins the Organization for Security Cooperation in Europe and some limited progress on CBMs in the ASEAN Regional Forum and the Organization of American States. In the UN, we are entering the seventh year of negotiation. There has been endorsement of general norms, the most important of which embed cyberattack in the existing framework of international law, including the law of armed conflict. However, there is no agreement to constrain use in wartime. Nor is there any agreement on the definition of a cyber weapon or on what would qualify as the use of force or armed attack in cyberspace. This is unlikely to change.

It is no longer it safe to discount the possibility of armed conflict between major powers, even if these conflicts might be limited in duration and scope or take forms to which we are unaccustomed. The increased level of international dispute means that cyberspace is a contested domain, where opponents maneuver to position themselves for advantage now and in the event of conflict.

In the last two hundred years, navies have gone from wooden ships to ironclads, from sail to steam, from big gun battleships to aircraft carriers and then guided missiles, from surface combat to undersea, air, and space. Each change has meant that to perform the maritime missions of protecting commerce, deterring attack, and establishing advantage at sea, navies must adjust and adapt.

We are in a period of experimentation with organizations, tactics and techniques to find ways to best use cyber capabilities in naval operations. The side that is best prepared to use the new technologies will have the advantage in both peacetime and war, and in the increasingly blurry area between the two. The challenge is to conceptualize the blend of EW, cyber, space, information and kinetic effect to create a new formula for partnership and superiority at sea.