Connecticut Debate Association

November 17, 2012

Amity Regional High School and New Canaan High School

Resolved: The United States should adopt a "no-first strike" policy for cyber warfare.

Cyberwarfare

From Wikipedia, the free encyclopedia

Cyberwarfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare[1] although this analogy is controversial for both its accuracy and its political motivation.

U.S. government security expert Richard A. Clarke, in his book *Cyber War* (May 2010), defines "cyberwarfare" as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[2]:6 The *Economist* describes cyberspace as "the fifth domain of warfare,"[3] and William J. Lynn, U.S. Deputy Secretary of Defense, states that "as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare . . . [which] has become just as critical to military operations as land, sea, air, and space."[4]

In 2009, President Barack Obama declared America's digital infrastructure to be a "strategic national asset," and in May 2010 the Pentagon set up its new U.S. Cyber Command (USCYBERCOM), headed by General Keith B. Alexander, director of the National Security Agency (NSA), to defend American military networks and attack other countries' systems. The EU has set up ENISA (European Network and Information Security Agency) which is headed by Prof. Udo Helmbrecht and there are now further plans to significantly expand ENISA's capabilities.. The United Kingdom has also set up a cyber-security and "operations centre" based in Government Communications Headquarters (GCHQ), the British equivalent of the NSA. In the U.S. however, Cyber Command is only set up to protect the military, whereas the government and corporate infrastructures are primarily the responsibility respectively of the Department of Homeland Security and private companies.[3]

In February 2010, top American lawmakers warned that the "threat of a crippling attack on telecommunications and computer networks was sharply on the rise."[5] According to The Lipman Report, numerous key sectors of the U.S. economy along with that of other nations, are currently at risk, including cyber threats to public and private facilities, banking and finance, transportation, manufacturing, medical, education and government, all of which are now dependent on computers for daily operations.[5] In 2009, President Obama stated that "cyber intruders have probed our electrical grids."[6]

…

In August 2010, the U.S. for the first time warned publicly about the Chinese military's use of civilian computer experts in clandestine cyber attacks aimed at American companies and government agencies. The Pentagon also pointed to an alleged China-based computer spying network dubbed GhostNet that was revealed in a research report last year.[37] The Pentagon stated:

> "The People's Liberation Army is using "information warfare units" to develop viruses to attack enemy computer systems and networks, and those units include civilian computer professionals. Commander Bob Mehal, will monitor the PLA's buildup of its cyberwarfare capabilities and will continue to develop capabilities to counter any potential threat."[38]

First strike

From Wikipedia, the free encyclopedia

In nuclear strategy, a **first strike** is a preemptive surprise attack employing overwhelming force. **First strike capability** is a country's ability to defeat another nuclear power by destroying its arsenal to the point where the attacking country can survive the weakened retaliation while the opposing side is left unable to continue war. The

preferred methodology is to attack the opponent's launch facilities and storage depots first. The strategy is called counterforce.

Overview

During the Cold War period, both superpowers, NATO and the Soviet Bloc, built massive nuclear arsenals, aimed, to a large extent, at each other. However, they were never used, as after a time, leaders on both sides of the Iron Curtain realized that global thermonuclear war would not be in either power's interest, as it would probably lead to the destruction of both sides, and possibly nuclear winter or other extinction level events. Therefore, at times, both sides refrained from deploying systems capable of unanswerable nuclear strikes against either side. However, in both nations, there were interests that benefited from the development and maintenance of first-strike weapons systems: what U.S. President Dwight Eisenhower termed the military-industrial complex; these forces encouraged the constant development of weapons systems of greater accuracy, power, and destruction. In addition, each side doubted the other side's commitment to not deploy first-strike weapons, or even in the event of their deployment, to not strike first. Some first-strike weapons were deployed; however like most nuclear weapons, they were never used.

Of the nuclear powers, only the People's Republic of China and the Republic of India have declarative, unqualified, unconditional no-first-use policies. In 1982, at a special session of General Assembly of United Nations, the USSR pledged not to use nuclear weapons first, regardless of whether its opponents possessed nuclear weapons or not. This pledge was later abandoned by post-Soviet Russia. The United States has a partial, qualified no-first-use policy, stating that they will not use nuclear weapons against states that do not possess nuclear weapons or other weapons of mass destruction.

Large scale missile defense systems are not first-strike weapons, but certain critics view them as first-strike enabling weapons. U.S. President Ronald Reagan's proposed Strategic Defense Initiative, if it had ever been deployed (and proven successful), would have undermined the fundamental premise of mutual assured destruction (the inevitable outcome of equal and unacceptable destruction for both sides in the event of nuclear war), removing the incentive for the US not to strike first.

These proposed defense systems, intended to lessen the risk of devastating nuclear war, would lead to it, according to these critics. Indeed, according to game theory, the side not building large-scale missile defenses would have an incentive to launch a pre-emptive first strike while such a strike could still get through.

No first use

From Wikipedia, the free encyclopedia

No first use (**NFU**) refers to a pledge or a policy by a nuclear power not to use nuclear weapons as a means of warfare unless first attacked by an adversary using nuclear weapons. The concept can also be applied to chemical or biological warfare.

As of October 2008, China,[1] India[2] and North Korea[3] have publicly declared their commitment to no first use of nuclear weapons.

NATO has repeatedly rejected calls for adopting NFU policy,[4] arguing that preemptive nuclear strike is a key option.[*citation needed*] In 1993, Russia dropped a pledge given by the former Soviet Union not to use nuclear weapons first.[5] In 2000, a Russian military doctrine stated that Russia reserves the right to use nuclear weapons "in response to a large-scale conventional aggression".[6]

The New Reality of Cyber War

Contributor: James Farwell and Rafal Rohozinski, Posted: 10/22/2012 www.defenceiq.com

The June 2012 report by New York Times chief Washington correspondent David Sanger that the Stuxnet cyber worm was only part of a broader operation, Olympic Games, launched against Iran by the United States and Israel affirmed what many suspected: cyber attack is not a distant theoretical probability. *(1)*

Stuxnet was the first alleged identified instance of weaponised computer code or malware employed as a 'use of force'. But it was not alone. Two other targeted computer viruses for espionage have surfaced: Duqu in September 2011, followed by Flame in May 2012. Media reports allege that both also targeted Iran.*(2)* As tools of espionage, use of neither would qualify as a use of force, but reflect new emphasis on cyber tools. Of the two, Flame drew wider attention. Apparently 20 times more complex than Stuxnet, Flame affected computers in Lebanon, the United Arab Emirates, the West Bank and Iran. It is said to have gathered intelligence by logging keyboard strokes,

recording conversations by activating microphones, and taking screen shots. At Iran's oil ministry and oil-export terminal, the virus also erased information on hard discs while gathering information.*(3)* Many attribute it to the United States and Israel. These allegations remained unconfirmed by either government.

A new era

These developments put the spotlight on a new era of international engagement. Israeli sources have long boasted about Israel's involvement in Stuxnet. The US/Israeli use of Stuxnet as reported in detail by Sanger has arguably created a new de facto norm for the conduct of cyber engagements other nations can follow or imitate. Previously, a key constraint on the use of software as a weapon has been the potential for legal liability arising out of collateral damage inflicted upon innocent parties not targeted. In practice, software can be narrowly targeted to surmount that challenge.

What Stuxnet shows is that it is possible to have the specific intended effect while avoiding or minimising unplanned side effects by clearly differentiating between the propagator, or boost-phase code that disseminates the program, and the actual payload code that creates the physical effect on a target (the distinction between the gift wrapping and the gift). The reported operation did apparently limit the scope of damage. Stuxnet shows that one can surmount concerns that malware would take down the global network, not just a specific target. The lesson is that cyber weapons are in a different category from nuclear devices, which have little practical use except as a deterrent.

The rules of conduct for the use of code are evolving. As parties develop more sophisticated capabilities and acquire experience in their use, the picture will grow more complicated and nuanced. The strategic situation contains echoes of the period between the two world wars, when rapid developments in new technologies and domains of war-fighting preceded an understanding of how effectively to employ them operationally. Tanks changed the way armies engaged in battle. But despite British and German experimentation with armour in the inter-war period, armoured tactics could only be proven and fully developed on the battlefield from 1939 onwards. There are, moreover, significant differences of view about whether the Germans, renowned for their blitzkrieg tactics, properly understood the strategic use of armour for manoeuvre warfare.

Reports that two states have employed code against another state against which war has not been declared undercuts the common view that risks of escalation render state-to-state cyber war implausible. Sanger reported that President George W. Bush, under whom Olympic Games was apparently initiated, desired that use of Stuxnet not violate the rules of armed conflict.*(4)* The Law of Armed Conflict does not prohibit damage to such critical infrastructure. But a strength of using code is that the targeting process can manage the risks.

Stuxnet may appear as embryonic as the British Mk.1 tanks that made their debut at the Battle of the Somme in 1916. But technology moves quickly. Modern states rightly fear cyber war. Evolving technology is accelerating the flow of information, placing unique pressures on decision-making. Responding to cyber attack may require making decisions at network speed using systems that are themselves targeted. The potential for cascading effects is amplified by the interconnectedness of cyberspace. Stuxnet worked leisurely. Future combat in cyberspace may be more akin to the global trading system than existing forms of kinetic engagement, and present a different strategic calculus.

Active defence versus first strike

As described by Sanger, Olympic Games puts into question the existing discourse over US doctrines of active defence versus offensive use of malware and the strategic communication employed to explain US actions. Nations have been rightfully unwilling to disclose their doctrines for the offensive use of cyber weapons. Open-source discourse has centred on delineating passive and active defence. No nation has been willing to declare its intent to use cyber weapons offensively for a first strike. But Stuxnet blurs the lines between what might constitute active defence and offense. It also moves the impact from the strictly cyber realm to one that may entail mechanical or physical damage.

Passive cyber defence is easiest to grasp. The notion includes firewalls, cyber 'hygiene' that trains an educated workforce to guard against errors or transgressions that can lead to cyber intrusion,*(5)* detection technology, 'honey pots ' or decoys that serve as diversions, and managing cyberspace risk through collective defence, smart partnerships, information training, greater situation awareness, and establishing secure, resilient network environments.*(6)* Active cyber defence is a more elusive notion. Industry operates under different legal constraints than the military and they view the notion of active defence differently. For industry, the notion includes working actively with private-sector partners to identify and interdict cyber intrusions. Action beyond that raises real concerns. Under US law causing more than $5,000 of damage to another computer is a felony.*(7)* US anti-trust*(8)* and privacy laws*(9)* raise other concerns. Yet private industry owns and operates 90% of US civilian critical

infrastructure. Its concerns will grow as future malware come into play, for current laws and operational capabilities provide inadequate defences.

The public sector operates under different rules. While private parties can take action unless prohibited by law, the military can act only within its prescribed authority. As a result, the military's notion of active defence remains unformed: no one is certain what it means or how to apply it. The Pentagon has made clear it would employ force to defend against cyber attacks.*(10)* But who has the authority to launch what actions, and under what circumstances? If a hostile force targets a naval cruiser for imminent attack, does the captain hold the authority to launch a preemptive attack? If he doesn't, who does? Should he try to move his vessel out of danger? What if he cannot? How can he 'actively' mount a defence?

US Cyber Command Chief General Keith Alexander has declared that 'a Commander's right to self-defence is clearly established in both U.S. and international law'.*(11)* He did not define what that entails. Would it include hot pursuit? Former US Air Force Secretary Michael Wynne has stated that US law allows 'hot pursuit' of criminals, enabling law enforcement to track and address cyber crime through the digital world.*(12)* That doctrine is well accepted in crime fighting,*(13)* but where it applies may hang on the status of an attacker. What rules govern may depend upon the status of an event as criminal activity, a military attack or a terrorist action.

Hot pursuit may well apply in cyberspace. Many concur that the law of the sea sanctions the use of the doctrine in the maritime domain,*(14)* which along with air, land, and space is viewed as a global commons. President Barack Obama has declared that cyberspace is also a 'recognized strategic commons'.*(15)*

A use of force?

For the most part the US discussion on cyber war has revolved around these notions of defence. But Olympic Games has apparently shown that the United States and Israel will use cyber weapons offensively.

The United States has previously said that its cyber strategies would respect international law. The key normative standards nest in United Nations Charter articles 2(4) and 51. Article 2(4) prohibits the 'threat or use of force against the territorial integrity or independence of any state'. Article 51 states that nothing 'in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations'.

But 'force' is not defined. There is no international convention that defines whether the use of software code should be deemed equivalent to the use of force. Cyber expert Herbert Lin has argued that the term almost certainly covers conventional-weapon attacks that injuring persons or irreparably damage property, but excludes economic or political acts (such as sanctions) that do not. In that view, Stuxnet would have constituted a use of force only if it had inflicted damage comparable to a kinetic attack, but it injured no one and the Iranians make no claim of irreparable physical damage.

But the US government apparently did view Olympic Games as a use of force. The strategic objective was not only to retard Iran's progress in developing nuclear weapons but to persuade Israel that using cyber weapons mooted the need for a kinetic attack on Tehran's nuclear institutions.*(16)* Both the G.W. Bush and Obama administrations strongly believed that Iran's nuclear-weapons programme had to be stopped. The United States has clearly felt a need to communicate that it would not tolerate Iranian intransigence. Former CIA Director Michael Hayden stated that:

> *This is the first attack of a major nature in which a cyberattack was used to effect physical destruction. And no matter what you think of the effects – and I think destroying a cascade of Iranian centrifuges is an unalloyed good – you can't help but describe it as an attack on critical infrastructure.(17)*

This implies that the Obama administration was willing in this case to affirm G.W. Bush's policy of pre-emption to deal with a threat deemed vital to national security interests, was willing to act in concert with a 'coalition of the willing' (even if the United States and Israel were the sole partners) to keep weapons of mass destruction out of the hands of rogue states,*(18)* and that this concern trumps commitments – including those expressed in the US 2011 Cyber Strategy,*(19)* to embrace multilateralism and partnership for cyber strategy.

It seems evident that the intent of Olympic Games was to irreparably damage critical infrastructure. The tenor of the operation and strategic intent – and Hayden's words – strongly imply that White House and Department of Defense lawyers considered the operation a use of force. The issue must have been considered. One can presume the answer the lawyers provided was affirmative.

Legally, did the White House exceed its jurisdiction either under the Constitution, which reserves to Congress the right to declare war, or under the War Powers Resolution of 1973?*(20)* It is hard to qualify Olympic Games as an act of war. US statute defines that as armed conflict, whether or not war has been declared, between two more nations or

between military forces of any origin.*(21)* It is significant that Iran has not suggested the use of Stuxnet constituted an act of war.

The War Powers Resolution offers a more nuanced issue. The resolution applies to the introduction of 'United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances'.*(22)* How does a nation use force except through military means? One can debate whether non-uniformed Stuxnet operations personnel qualify under the notion of distinction as combatants, but one can make a strong argument that Olympic Games fell under the ambit of the resolution. Presumably the response is that it constituted a covert action that did not trigger the operation of the law.

Given that the objective was to destroy an enemy's critical war-fighting capacity, though, one might wonder whether the logic in avoiding the jurisdiction of the resolution – or Congress's power to declare war – would apply to a modern Pearl Harbor. The air war in Libya may offer a clue to policy mindsets. Denying any obligation to ask Congress for authorisation to act, the Obama administration argued that 'U.S. operations do not involve sustained fighting or active exchanges of fire with hostile forces, nor do they involve ground troops'.*(23)* Similarly, Stuxnet did not involve armed fighting or exchanges of fire with hostile forces, although future engagements may focus debate on what constitutes armed forces. That cyber weapons often do not entail uniformed individuals firing rockets, dropping bombs, or firing guns does not, looking over the horizon, inherently render its users non-combatants.

What if Iran decided to respond kinetically? How does that alter the authority of the White House to continue a programme? Stuxnet was a fire-and-forget weapon. Although code can be designed to hit a specific target, in practice, once launched, there was no control over the consequences it inflicted – or upon whom. Indeed, Sanger reported that American officials were quite unhappy when Stuxnet got loose on the Internet.*(24)* The operational environment in war is random. The collateral effects of a cyber weapon add a new dimension to that challenge. One must think beyond the Iranian situation. What if Congress wanted a president to cease an operation that could not be terminated? Olympic Games side-stepped the problem, but hardly obscures the need for future strategic thinking.

Whether there was use of force raises other issues. Olympic Games involved a pattern of engagements. One must consider the larger implications of an individual event. Does a pattern convert employment of cyber weapons into a use of force? The answer isn't clear. The unpredictable nature of damage that cyber attack can inflict may require a new definition of war.

Intent may also matter in determining whether an engagement constituted a use of force. Open-source reporting indicates that any damage inflicted on the Natanz uranium-enrichment facility was temporary and reparable. But that was not the intent. What if someone dropped a bomb on London or New York that failed to detonate? Isn't that a use of force – or possibly, depending on the facts, an act of war? Deciphering intent may pose a challenge, but in law it may be objectively inferred. The case of unexploded ordinance seems easier to grasp, but how deep is the distinction between that and a cyber worm that fails? This issue needs debate and should enter future strategic calculations.

Finally, did Article 51 of the UN Charter justify Olympic Games? Like 'force', 'armed attack' remains undefined, even where force is clearly employed. Certainly the implications of new technologies for Article 51 or other international conventions remain unclear. This consideration matters enormously to Israel, which contends that a nuclear first strike would destroy the nation, preventing or mooting a response. Washington worries about Israeli security, but also a potential and de-stabilising Middle East arms race should Iran acquire a nuclear weapon.

Strategic implications

The use of malware by state actors has altered the realities of cyber attack. History teaches that once weapons technology becomes feasible, states deploy it. Today the world may confront a dangerous technology race characterised by rapidly evolving and lethal weapons.

Clausewitz believed that in warfare, the advantage rested with the defence. Cyber reverses that equation. It also offers the potential to build the fog of war through the ability to effect disruption, deception, confusion and surprise. We are only beginning to envisage the potential for different forms of malware, or the strategies or tactics employed to use it.

A cyber-security tool may require millions of lines of code and a complex system to track and identify events. Malware requires a lot less. Computer code can be designed to evolve rapidly, mutating faster than defences can be mustered. Code can be highly targeted. It can leverage social and technological vectors. It can render a cyber defence obsolete within seconds. It can overwhelm a system that may have taken years to construct. Clausewitz believed that the advantages enjoyed by defence required that an offense employ greater resources. Cyber reverses

that equation. Nations may now shift away from a refusal to use cyber weapons for first strike. That in and of itself complicates both offensive and defensive strategies.

Although some have argued that Olympic Games lowered the threshold for the use of cyber weapons, it may in fact actually raise it. States may recognise a higher responsibility to design weapons that offer strong assurance of striking only the intended targets. That was the intent of Stuxnet's planners and designers. But matters could have worked out much differently. Robert Burns was right: the best laid plans of mice and men often go awry.

Stuxnet shows that creating effective malware turns on imagination, technical expertise and ingenuity. But to deliver code as a warhead also requires highly specific domain experience and superior intelligence capabilities that often only states possess. Our view is that malware is not a wide-area weapon. As it evolves, it will be used narrowly to attack particular targets and to generate specific shaping effects.

Olympic Games raises the veil on key strategic implications. Stuxnet aimed to destroy a specific capability. But it importantly illustrates the political nature of war. Achieving a strategic political objective does not necessarily require destroying an enemy. Olympic Games was devised when G.W. Bush pushed for an alternative to the unpleasant choice between allowing Iran to develop a nuclear-weapons capability or halting the programme through kinetic attack. The cyber programme bought time in which to employ punishing sanctions and to signal to Iran that other nations would not tolerate an Iranian nuclear-arms programme. The lesson is that cyber weapons may offer non-kinetic ways to disrupt an operational capability of an adversary.

Future cyber weapons will similarly aim to constrain the ability of an adversary to manoeuvre, coordinate or synchronise, and to divert enemy commanders from focusing on the achievement of their own objectives. Stuxnet succeeded splendidly in creating confusion. Sanger reports that Iranians came to distrust their own instruments. The idea, he quotes one source, 'was to mess with Iran's best scientific minds' and 'make them feel they were stupid'.*(25)*

Conceptually, unsettling the consciousness of an adversarial commander, or a CEO or government official, causing a loss of belief in his ability to control events and depriving him of control, helps disrupt an adversary's ability to fulfil its objectives. Stuxnet's creators merit high marks for recognising the value of that goal. While the final result fell short, open-source reporting indicates that Stuxnet did retard Iranian progress.

As reported in open sources, Olympic Games exemplified an operation intended to reduce the resistance of a rival system and to inflict attrition upon its resources. Destruction of an asset is one of many potential objectives that cyber weapons can achieve. Future cyber weapons may disrupt communications systems or the ability of adversaries to cohesively operate air, naval or ground forces. They could slow the speed at which an adversary is able to mass forces or deploy assets, destroying precious momentum vital for an adversary's offense.*(26)* Indeed, smart strategy is often less about destroying an enemy than paralysing command and control, and neutralising an adversary's operational ability.

One unfortunate development has been the leaks from Washington and Israel (where sources have long claimed credit for Stuxnet) about Olympic Games. These present a strategic challenge. An obstacle confronting any nation that wishes to retaliate against a cyber intrusion is the need to identify the intruder. The leaks solved that problem for Iran, and opened the United States and Israel to potential counterpunches that would entail far less stigma for Tehran than action against a putative attacker whose guilt could not be confirmed.

Finally, it is worth noting that the weapons employed by Olympic Games are largely indistinguishable from the technology that cyber criminals employ. That will make international treaties and conventions aimed at limiting cyber crime more difficult to secure. The utility and effectiveness of these weapons for national-security interests may trump policy considerations that favour better global policing of cyber crime.

There has been a widespread view that criminal entrepreneurs or state-sponsored proxies, acting at arm's length to insulate states from culpability for their policies, would emerge as the real challenges in a cyber era in which one individual can change the way the world does business. But now it seems that state-to-state engagement, whether or not it meets the conventional definitions of the use of force or an act of war, will define a new reality and require new strategic calculations. The discourse arising out of reports about Olympic Games underscores why the United States and other countries should engage in a transparent debate over whether or how cyber weapons should be employed. Every nation – including civilian as well as government institutions – must develop strategies to address these new realities.

This article first appeared in *Survival: Global Politics and Strategy*, vol. 54, no. 4, August–September 2012, pp. 107-120.

When is a cyberattack an act of war?

Nakashima, Ellen. **The Washington Post** 28 Oct 2012: B.1

On the night of Oct. 11, Defense Secretary Leon Panetta stood inside the Intrepid Sea, Air and Space Museum, housed in a former aircraft carrier moored at a New York City pier, and let an audience of business executives in on one of the most important conversations inside the U.S. government.

He warned of a "cyber Pearl Harbor," evoking one of the most tragic moments in American history, when Japanese bombers unleashed a devastating surprise attack on a U.S. naval base in Hawaii on Dec. 7, 1941, killing 2,402 Americans and wounding 1,282 more. President Franklin D. Roosevelt called it "a date which will live in infamy" as he asked Congress for a declaration of war.

Sixty years later, another surprise attack killed almost 3,000 people when al-Qaeda terrorists flew two jetliners into New York's twin towers. Panetta cited the Sept. 11, 2001, strikes, too, warning that the United States is in a "pre-9/11 moment," with critical computer systems vulnerable to assault.

We all know what an act of war looks like on land or sea, and by evoking two of the most searing attacks in our modern history, Panetta was trying to raise a sense of urgency about the threat in a new domain made of bits and bytes zinging between servers around the world.

But what does an act of war look like in cyberspace?

And perhaps more important, what does the U.S. government do when cyberattacks fall short of that - assuming it can identify the perpetrators in the first place?

What about something like Shamoon, the nickname for a virus that wiped data from 30,000 computers at Saudi Arabia's state-owned oil company in August, affecting business operations for two weeks? Panetta called that assault, along with a similar strike on Qatar's RasGas, "probably the most destructive attack" on the private sector to date. Another U.S. official declared it a "watershed" moment, beyond the troubling but all-too-familiar thefts of data and disruption of Web sites.

Unlike the Japanese planes at Pearl Harbor, the virus had no telltale markings that gave away its origins. The U.S. intelligence community has privately concluded that the invader was sent by Iran, though some security experts outside the government say they have reason to believe thatIran was not the perpetrator.

If Tehran is responsible, what was its motive? In the view of intelligence officials, it was striking back for sanctions; for the Saudi kingdom's implicit support for an oil embargo; and for the damage done to Iran's nuclear program by Stuxnet, the nickname for a cyber-sabotage campaign by the United States and Israel to slow the country's pursuit of a nuclear weapon by damaging almost 1,000 uranium-enrichment centrifuges.

The Shamoon attack on Saudi Aramco did not cause enough physical damage to rise to what international law experts call an armed attack. But what if something like it happened to several energy companies in the United States and it could be traced conclusively to a foreign government or a terrorist group? How much damage, pain and fear would need to result before national security officials would say, "We can't let this go unanswered"?

If government officials have reached a consensus on those questions, they're keeping it to themselves.

Welcome to the new world of "drip, drip cyber attacks," in the words of Tufts University law professor Michael J. Glennon. The nature of cyberspace, he says, creates the potential for "a mysterious airliner accident here, a strange power blackout there, incidents extending over months or years," generally "with no traceable sponsorship."

Japan's attack on Pearl Harbor was a direct assault on a U.S. military installation. But much of the nation's critical computer networks belong to the private sector. The companies that provide transportation, water, telecommunications and energy could become targets for adversaries bent on destruction. That simple fact has led to a complicated set of questions for policymakers responsible for the nation's security.

Should the U.S. government step in to prevent a destructive cyberattack, if it can see one coming, aimed at the private sector? If not, and such an assault is successful, when should Washington retaliate and how, assuming the attack can be conclusively traced to another nation or to a terrorist group? When should the government make preemptive use of cyberweapons to alter a state's agenda or behavior?

If a major cyberattack happened - a computer virus knocking out air traffic control, for instance, and sending planes crashing to the ground - the president and the National Security Council would focus first on what type of response would be proportionate, justified, necessary and in the U.S. interest. It might be a military response. It might be a cyber-response. It might be naming and shaming the attacker before the United Nations. It might be imposing sanctions. It might be no response at all.

Deciding what amounts to an act of war is more a political judgment than a military or legal one. International law avoids the phrase in favor of "armed attack" and "use of force." Retired Gen. James Cartwright, former vice chairman of the Joint Chiefs of Staff, has often said that an act of war "is in the eye of the beholder."

As Cartwright has pointed out, the United States didn't go to war with North Korea after it sank a South Korean warship in 2010, nor with Iran after the U.S. Embassy in Tehran was seized in 1979. Would we want to start a war over a virus that causes a power blackout? And if not, what other actions might the government contemplate?

The government has defined an armed attack in cyberspace as one that results in death, injury or significant destruction, as Harold Koh, the State Department's chief legal adviser,recently put it. Here's the rule of thumb, as Koh stated it: "If the physical consequences of a cyberattack work the kind of physical damage that dropping a bomb or firing a missile would, that cyberattack should equally be considered a use of force." If an attack reaches those levels, then a nation has a right to act in self-defense.

The more difficult cases will look something like what happened to Saudi Aramco. Matthew Waxman, a Columbia University law professor who studies the strategic dimensions of cyberattacks, said economic damage alone traditionally does not give rise to a right of self-defense. While "the erasure of data . . . is expensive to replace," he said, "I would not call that an armed attack."

A more complicated scenario: a cyber-assault on Wall Street computers that sends the markets into a tailspin and causes ripple effects throughout the economy. Industry experts say such an attack would be difficult to pull off - it's one of those low-probability, high-consequence events government officials fear.

"I can see that rising to the level" of an armed attack in some people's minds, Waxman said, but others would say it falls short of physical damage or loss of life.

Senior policymakers have been wrestling with these very issues. And the Saudi Aramco attack has heightened the sense of urgency, making the threat all the more concrete. "This was a deliberately disruptive event, done on purpose, not by some rogue hacker. Not some out-of-control operative," said one U.S. intelligence official.

Panetta, in his speech, said, "If a crippling cyberattack were launched against our nation, the American people must be protected." But what is "crippling"? What exactly would the military do to ensure such protection? That discussion remains very much behind closed doors, where the government has been working on rules of engagement that would guide its response.

A senior defense official, in an interview, said officials have done a lot of work on how the government would respond to certain attacks. "We feel we're very prepared to answer that question if it should come up in the case of the United States," he said.

But he would not get into specifics, for instance, as to whether destruction of data that caused a drop in the stock market or a huge increase in gas prices would trigger a military or any other response.

"Those are always classified things," he said. "It's not helpful to the United States to give a road map to the enemy to know when something is an attack on the nation and when it is not."

His point: Why tell other nations what the United States is willing to tolerate before it will respond forcefully?

The severity and duration of effects - the amount of pain caused - is only one element that drives decisions about how to respond. Perhaps the more difficult factor is figuring out who is behind an attack - and why.

U.S. officials believe that factions of Iran's Revolutionary Guard Corps were behind the attacks on Saudi Aramco and RasGas and that the Iranians were sending a message to the West and its supporters:You unleashed the Stuxnet virus on our nuclear program, and we're firing back.

"They don't see it as an escalation," the U.S. intelligence source said. "They see it as a response to what was done to them: 'Hey, you did it to us, and we're going to come back at you.' "

U.S. officials have not blamed Iran - or any other nation or group - publicly for the Aramco and RasGas attacks. An earlier version of Panetta's speech blamed the attacks on a "state actor," according to one source, but that language was cut.

There is another school of thought, coming from outside the government, that the attack was carried out by a group of employees, some of whom may no longer work there, and non-employees with a grudge against the company and the Saudi government. None has any apparent link to Iran, these sources assert.

No one, however, is making their case publicly or offering evidence to prove their conclusions. That, too, is the nature of drip, drip warfare.

The United States and the world may be moving toward a greater strategic use of cyberweapons to persuade adversaries to change their behavior. This can be good, if it averts war. On the other hand, it could cause other nations to feel vulnerable. Some experts foresee a kind of cyber arms race as nations try to catch up.

Cyber-sabotage, by nature, doesn't seem as cataclysmic as the Pearl Harbor or Sept. 11 attacks. But that may change. As Panetta warned in his New York speech, "These attacks mark a significant escalation of the cyberthreat, and they have renewed concerns about still-more-destructive scenarios that could unfold."

Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials

By SCOTT SHANE, The New York Times, September 26, 2012

WASHINGTON — For years, even as the United States carried out sophisticated cyberattacks on Iran's nuclear program and the Pentagon created a Cyber Command, officials have been hesitant to discuss American offensive cyberwarfare programs openly. Since June, in fact, F.B.I. agents have been investigating leaks to The New York Times about the computer attacks on Tehran.

But the reticence is giving way. The chorus of official voices speaking publicly about American cyberattack strategy and capabilities is steadily growing, and some experts say greater openness will allow the United States to stake out legal and ethical rules in the uncharted territory of computer combat. Others fear that talking too boldly about American plans could fuel a global computer arms race.

Next month the Pentagon's research arm will host contractors who want to propose "revolutionary technologies for understanding, planning and managing cyberwarfare." It is an ambitious program that the Defense Advanced Research Projects Agency, or Darpa, calls Plan X, and the public description talks about "understanding the cyber battlespace," quantifying "battle damage" and working in Darpa's "cyberwar laboratory."

James A. Lewis, who studies cybersecurity at the Center for Strategic and International Studies in Washington, says he sees the Plan X public announcement as "a turning point" in a long debate over secrecy about cyberwarfare. He said it was timely, given that public documents suggest that at least 12 of the world's 15 largest militaries are building cyberwarfare programs.

"I see Plan X as operationalizing and routinizing cyberattack capabilities," Mr. Lewis said. "If we talk openly about offensive nuclear capabilities and every other kind, why not cyber?"

Yet like drone aircraft, which similarly can be used for both spying and combat, American cyberattack tools now are passing through a zone of semisecrecy, no longer denied but not fully discussed. President Obama has spoken publicly twice about drones; he has yet to speak publicly on American cyberattacks.

Last week, at a public Cyber Command legal conference, the State Department's top lawyer, Harold H. Koh — who gave the Obama administration's first public speech on targeted killing of terrorists in 2010 — stated the administration's position that the law of war, including such principles as minimizing harm to civilians, applies to cyberattacks.

In August, the Air Force raised eyebrows with a bluntly worded solicitation for papers advising it on "cyberspace warfare attack capabilities," including weapons "to destroy, deny, degrade, disrupt, deceive, corrupt or usurp" an enemy's computer networks and other high-tech targets.

And a few weeks earlier, a top Marine commander recounted at a public conference how he had used "cyber operations against my adversary" in Afghanistan in 2010. "I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire," said Lt. Gen. Richard P. Mills, now deputy commandant of the Marine Corps.

Cyberwarfare was discussed quite openly in the 1990s, though technological capabilities and targets were far more limited than they are today, said Jason Healey, who heads the Cyber Statecraft Initiative at the Atlantic Council in Washington.

"Our current silence dates back 8 or 10 years, and N.S.A. is a big reason," said Mr. Healey, who is working on a history of cyberwarfare.

The National Security Agency, which plays a central role in Cyber Command, traditionally breaks foreign codes and eavesdrops on foreign communications; it is among the most secretive agencies in government. Years ago it pioneered the field of cyberespionage: breaking into foreign computer systems in order to collect intelligence. The same skills and reflexive secrecy of spies carried over to cyberwarfare, Mr. Healey said. American officials have long preferred to talk cyberdefense, leaving the attack side in the shadows.

The increased candor recently about cyberoffense results not from a policy change, officials say, but from an inevitable acceptance of attacks on computer networks as a standard part of military and intelligence capabilities. The fact that dozens of Beltway contractors see cyberwarfare as one of the few parts of the defense budget that are likely to grow is also a factor.

When Darpa announced a "proposers' day workshop" for its Plan X program, the "overwhelming response from industry and academia" led the defense research agency to expand the event to an extra day, the agency said in a statement. (A Darpa spokesman declined to comment further on Plan X.)

Just as drone-fired missiles have never been a secret to those on the ground, so cyberattacks have consequences that cannot be hidden, even if their origin may be initially uncertain. The computer worm called Stuxnet, devised by the United States and Israel to destroy Iran's nuclear centrifuges, was quickly detected by computer security experts when it infected networks around the world in 2010 — but remains highly classified.

Hence the Cyber Command legal conference, which avoided specific cases while dwelling on principles. Mr. Koh, of the State Department, told the conference that the United States carries out "at least two stages of legal review" on cyberwarfare operations — considering whether the law of war prohibits the use of "new weapons" altogether and, if not, how the law governs their use in "each particular operation."

Matthew Waxman, a law professor at Columbia and former Defense Department official, said speaking openly about cyberwarfare policy was important because it allowed the United States to make clear its intentions on a novel and fast-emerging form of conflict.

Because both the Bush and Obama administrations were slow to speak publicly about their use of armed drones, Mr. Waxman said, "they ceded a lot of ground to critics to shape the narrative and portray U.S. practices as lawless." As a result, he said, "the U.S. is trying to play catch-up, giving speech after speech, saying 'We abide by the law.' "

Now, Mr. Waxman said, because the United States "occupies a position of advantage on offensive cyber capabilities, it should seize the opportunity to lay out a set of rules for itself and others."

That is a worthy goal, said Daryl G. Kimball, executive director of the Arms Control Association. But he said that came with a hazard: more talk about the United States' cyberwarfare capabilities might prompt other countries to step up their own programs at a time when the world is "on the cusp of a cyber arms race," he said.

Mr. Kimball said Darpa's sweeping public statement about the goals of its Plan X for cyberwarfare might be a case in point.

"It makes it sound like the U.S. is preparing to be able to wage a full-out cyberwar," Mr. Kimball said. "Those kinds of statements could come back to haunt the U.S. down the road."

Pentagon's Plan X: how it could change cyberwarfare

Mulrine, Anna. **The Christian Science Monitor** [Boston, Mass] 12 Oct 2012: 12

The same Pentagon futurologists who helped create the Internet are about to begin a new era of cyberwarfare.

For years, the Pentagon has been open and adamant about the nation's need to defend itself against cyberattack, but its ability and desire to attack enemies with cyberweapons has been cloaked in mystery.

Next week, however, the Pentagon's Defense Advance Research Products Agency (DARPA) will launch Plan X an effort to improve the offensive cyberwarfare capabilities needed to dominate the cyber battlespace, according to an announcement for the workshop.

Though the program will be closed to the press, the relatively public message is a first for the Pentagon. For one, it shows that the Pentagon is now essentially treating its preparations for cyberwar the same way it treats its preparations for any potential conventional war. Just as it takes bids from aerospace companies to develop new jet fighters or helicopters, Plan X will look at bids from groups that can help it plan for cyberwarfare and expand technologies.

Moreover, it opens a window into the highly secretive world of offensive cyberwarfare. No longer is it unclear whether the US is in the business of planning Stuxnet-style cyberattacks. Plan X indicates that such capabilities which experts say could range from taking out electrical grids to scrambling computer networks in top-secret facilities to causing the pacemaker implanted in an enemy official to go haywire will be an explicit part of the military playbook.

If we can have a robust public discussion of nuclear weapons why not a robust discussion of cyberstrategy? says Jim Lewis, director of the Technology and Public Policy program at the Center for Strategic and International Studies in

Washington. Up until now, cyber has been kind of ad hoc. What theyre doing now is saying that this is going to be a normal part of US military operations.

The US is already engaged in offensive cyberwar. Media reports claim that the US helped develop and deploy the Stuxnet digital worm, which inflicted serious harm on Irans uranium enrichment program.

In his most wide-ranging speech to date on cyber warfare Thursday, Defense Secretary Leon Panetta hinted at the need for increased offensive capabilities, warning that America wont succeed in preventing a cyber attack through improved defenses alone.

If we detect an imminent threat of attack that will cause significant physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us, to defend this nation when directed by the president, Mr. Panetta said. For these kinds of scenarios, the department has developed the capability to conduct effective operations to counter threats to our national interests in cyberspace.

But the lack of discussion surrounding offensive cyber capabilities and a clear US military plan for pursuing them has been a significant roadblock for US military forces interested in honing those skills, says retired Col. Joe Adams, a former West Point professor who coached the military academys cyber team.

In the past there has been a skittishness about teaching cadets offensive skills like how to hack into systems, says Dr. Adams, now executive director of research and cybersecurity for Merritt Network, Inc. Weve really ramped up the defensive part, but there hasnt been any work done to identify people who have the intuitive ability to conduct operations on the offensive side.

Many of the threats the US faces and may in turn inflict on other countries and non-state actors will be nuanced.

The notion of a cyber Pearl Harbor, as Panetta has characterized it, is a misnomer, Adams adds.

Everybodys looking for a cyber Pearl Harbor we dont need a Pearl Harbor to really mess things up. Thats the very nature of this advanced, persistent threat: Were not kicking peoples doors in anymore.

Instead, cyber incursions will be more subtle. Just imagine what could happen in a hospital, Adams says. I dont even have to turn off the refrigerators. I just have to change the thermostat so theyre too warm, or too cold, or make some blood supplies go bad, or spoil a little medicine, or just reroute where they send ambulance alerts.

In particular, offensive cyberskills are more art than science, says Adams. These kids need to be screened right, and they need to be utilized. A career path in the military is built on building their skills, but also retaining them. Weve done really poorly with that.

Part of the problem is that American military training has long emphasized traditional skills, which are often are at odds with developing cyber warriors. You could have an outstanding cyberthinker in a class, but tradition dictates that hes going to be a tank platoon leader, or a rifle platoon hes going to have to prove himself as an Army officer before theyre going to make use of his talent, says Adams.

In the meantime, his cyberskills atrophy. The cadets I was teaching, there just wasnt another outlet for them in the military yet.

Plan X is designed to help the Pentagon understand the cyber battlespace and to develop skills in visualizing and interacting with large-scale cyber battlespaces, according to the DARPA proposal.

These, too, are unique skills that must be cultivated within the military, says Adams. Another art piece is mapping a network [that could be a potential target]. How do you do it and how do you do it subtly without knocking things over and turning things off? And if its hostile, how do we do it without getting caught?

Plan X hints at some of these needs and makes it clear that the Pentagon is grappling with how to establish a framework for fighting cyberwar, too.

Plan X is an attempt by the national security bureaucracy to come to grips with the multitude of issues around use of cyberweapon in an offensive form the legal, diplomatic, ethical issues, says Matthew Aid, a historian and author of "Intel Wars: The Secret History of the Fight Against Terror."

We cant have a public discussion about Stuxnet, about these brand new weapons or their ethical implications until the White House pulls back just a little the veil of secrecy that surrounds the entire program, Mr. Aid adds.

For example, Stuxnet revealed how unwieldy such weapons can be when it inadvertently jumped into friendly computer systems that were never meant to be targeted.

Indeed, One of the biggest problems in cyberwarfare is the potential for collateral damage, says Mr. Lewis of the Center for Strategic and International Studies.

You just can't attack stuff and not worry that innocent civilians will be harmed you have to take steps to mitigate the risk.

Aid says now is the time to have these conversations. We can only see one tenth of one percent lurking beneath the surface whats beneath the surface scares ... me," he says. "This is combat this is war by a different name.

The Pentagon has always been secretive about its desire and ability to carry out offensive cyberwarfare. Now, Plan X makes it clear that offensive cyberattacks will be in the Pentagon playbook.

A Brave New World of War: Cyber Warfare & Defense in Depth

Huffington Post, 10/15/2012 5:59 pm

Last week the U.S. Secretary of Defense, Leon Panetta, warned of a possible cyber "Pearl Harbor" attack on the U.S. He called attention to a new battle space: cyberspace.

This speech appeared to have several targets and we can draw several conclusions from it. First, and easiest to discern, is that Panetta is rousing the U.S. Congress to take concrete action and pass into law rules and regulations governing the sharing of information between private enterprises and the government. Many might recall the protests this last spring over the Cyber Intelligence Sharing and Protection Act (CIPSA), and this clarion call from Panetta appears to be harkening back to these same issues. Indeed, this is probably why he explicitly notes that the President is likely to issue an Executive Order should Congress fail to act.

The second target is the American, and perhaps international, audience. With much speculation about the U.S.' potential cyber threat and its response capability, it is high time someone higher up actually address it. While the White House has most certainly put forth documentation regarding its position regarding cyber security, little from the defense community has been forthcoming. Panetta's speech, therefore, unveiled many more specifics than the U.S.' International Cyber Security Strategy, which for the most part aims at such lofty goals as providing for the free flow of information while simultaneously ensuring security of networks.

The final, and to me the largest, target is the potential cyber adversary. Since much pertaining to cyber capability and warfare is classified, the decision for Panetta to show the U.S.' hand is telling. Allow me to explain. Much ink has been spilt over the "attribution problem." This problem states that cyber attacks are very difficult to trace with absolute certainty, and so attributing responsibility to one or more parties is more of a guessing game than anything. Because the issue of attribution calls into question whether we can know with 100% certainty whether an attack came from, say Russia, China, Iran, Lichtenstein, or the Moon, any attempt to either retaliate in self-defense or punish for deterrent effects will be problematic at best. What if we picked the wrong state? What if the cyber-warriors were so talented that they made it appear that it was China attacking and really it was Botswana? We might end up attacking an innocent third party, thereby becoming an aggressor ourselves. But Panetta's speech clears away the uncertainty surrounding the attribution problem. He stated that the "United States has the capacity to locate [the aggressors] and to hold them accountable for their actions." Wow. That is some serious stuff.

What it means is that the U.S. has very good cyber forensic capabilities and that it has probably procured enough consensus from private internet providers to share critical information regarding cyber attacks. What this also means is that the U.S. will not only know who attacked it, but it will use *any means* it sees fit to either preempt the attack or act to deter potential attackers in the future. That means both cyber and traditional (or sometimes called 'kinetic') warfare is on the table. Most telling still is that the U.S. has marked out three areas where it will act if provoked or attacked: the nation, the national interest, and allies.

Acting to defend the nation is rather unsurprising. Acting to defend national interest(s) is also, given U.S. military and foreign policy history, unsurprising. What does seem surprising, though, is the bit about the allies. The potential here is that if a North Atlantic Treaty Organization (NATO) ally is attacked by a cyber weapon, then the U.S. might retaliate with either cyber or traditional weapons on the ally's behalf. This statement appears to contradict, or at least militate against, earlier NATO findings about cyber attacks against Estonia in 2007.

All in all, Panetta's statement is a clear warning: cyber war is here and the U.S. is prepared to enter the fray with whatever means necessary. The questions for us, now, are what should we do about it? Certainly public rules of engagement should be made available, but more than that, transparency in the policy and governance processes is also a must. It is a must because the greatest weapon a cyber warrior has is a weakness in computer code. If there is no weakness, then there can be no attack. If we make cyber security a common good -- governed by the commons -- than we have more minds at work to secure networks, and this can only be done outside of the shadows.