PEPPERDINE UNIVERSITY

Global Tides

Volume 2 Article 3

2008

Bytes and Bombs: Information Warfare and Accidental Nuclear War

Nicholas Stewart
Pepperdine University

Bytes and Bombs: Information Warfare and Accidental Nuclear War

Nicholas Stewart

Abstract

While both information warfare and accidental nuclear war have been discussed in detail in academia, their intersection has long been ignored. Information warfare can be used to create animosity between states and could even spark war during times of crisis. Furthermore, not all states benefit from the technology advances of the first world: nations like Russia and Pakistan have disturbing gaps in their nuclear command and control that could be easily exploited by other states, internal factions or even terrorist organizations. Comparing the information vulnerabilities of the United States, Russia and Pakistan, one can only conclude that immediate action is needed to prevent a possible accidental nuclear war.

> There are but two powers in the world: the sword and the mind. In the long run, the sword is always beaten by the mind.
>
> -Napoleon Bonaparte

The world is getting smaller. With the amazing popularity of the internet and the ability for almost anyone to receive information and communicate across the globe, the world is shrinking. While there is no end to the good that the Internet and the spread of information are causing, this technology presents a new political and military defense challenge to leaders:

> Information age technology is making the environment in which future military operations occur more dynamic and unpredictable. It renders national economies sensitive to global developments, heightens cultural and political awareness on the part of the world's populations, and fuels radical movements that promote worldwide political fragmentation and destabilization.[1]

With information technology being used extensively by governments, a possibility arises for the manipulation or use of information technology channels for nefarious purposes, such as conflict or war.

Information warfare, or "infowar", is a broad and vague topic. For the purpose of this discussion, information warfare can be defined as "activities by state or non-state actors to exploit the content or processing of information to its advantage in time of peace, crisis, or war, and to deny potential or actual foes the ability to exploit the same means against itself."[2] This can be anything from hacking into an enemy's computer system and manipulating programs, to the dissemination of false news reports about one's own military capabilities or intentions. The objectives of infowar are just wide ranging from use during a conventional military conflict "to deny enemy forces battlespace awareness and to obtain dominant awareness for oneself,"[3] to use by terrorist organizations to destroy a country's network without regard for the result.

There is no doubt that information warfare can be used to influence government perceptions and policies, but what happens when nuclear weapons are thrown into the mix? The next war or conflict will not emerge or be fought on the land, air, or sea, but

on information networks and the nations of the world are unprepared. The chance that this weakness might be exploited is high and raises the possibility that infowar could create or magnify the conditions under which an accidental nuclear war might occur.

History of Information warfare

> The mind is the greatest weapon.
>
> -John Rambo

Information strategies in warfare are as old as war itself. In the Third Century B.C. during the Second Punic War, Hannibal used observers stationed on hilltops to track Roman troop movements allowing for his forces to destroy Roman armies twice the size of his own.[4] The Mongols in the Thirteenth Century A.D. used a system of "arrow riders" to communicate over their vast empire. This kept Genghis Khan and his generals constantly updated. This allowed the Mongols to defeat adversaries that outnumbered their forces maintaining control of their empire for over a hundred years.[5] More modern tactics of information warfare emerged in 1798 when the British victoriously used their naval forces to cut off communication between Napoleon's expedition force in North Africa and the main forces and supplies in Europe. A few years later, a lone British frigate employed this strategy with spectacular success when it was able to terrorized the French Navy by destroying its communication stations and engage in guerrilla warfare tactics to pick off French forces.[6]

Modern information conflict strategies take on a similar but more global pattern: in the 1990's several large and popular websites were temporarily shut via "denial of

service" attack, which uses a group of computers to constantly request information from a website overloading its servers.[7] Another example is US and Chinese civilians recently engaging in cyberwarfare. In 1999, when NATO mistakenly bombed the Chinese embassy in Belgrade, Chinese hackers took down or defaced several US government websites. In 2001, after the Chinese downing of a US spy-plane, US hackers attacked Chinese censuring routers and defaced government websites.[8] A final example occurred in April 2007 when Estonia was subject to the first case of outright cyberwar. In response to the moving of a Russian World War II monument on the eve of a Russian victory celebration, Estonian government, banking, news, university and police internet systems were crippled by Russian hackers 128 separate instances. The attacks seemed to be in coordination with the Russian government expressing hostilities (such as shutting down the bridge connecting the two countries) and were highly organized. Many of the attacks were traced back to Russian government computers and even some systems in the office of President Putin.[9]

An Eagle with Clipped Wings--American Infrastructure Weaknesses

As shown by past incidences, the US is not immune to infowar or cyberwar strategies, but the weaknesses go far beyond defacement of websites:

> Perhaps U.S. vulnerabilities to such convergence were best dramatized during a 1997 Joint Chiefs of Staff exercise, code-named Eligible Receiver. The exercise was intended to test the United States government's ability to respond to cyber attacks. The results opened

> the eyes of a number of skeptics. Using software widely available from hacker web sites, the 35-man team (red team) of attackers proved that they could disable elements of the U.S. electric power grid (through the SCADA systems) as well as incapacitate portions of the military command and control systems in the Pacific and Emergency 911 systems in the United States.[10]

It is worth noting that "Eligible Receiver" had restrictions that kept it from illustrating the full range of holes in American information security, specifically that team members could only use software that was available to the public and were not allowed to break any laws.[11] Thus one can only imagine what could happen to U.S. infrastructure when attacked by hackers that use custom programs and hold no legal restrictions. U.S. government networks are highly vulnerable. The U.S. House Oversight and Government Reform Committee revealed that in 2006 the federal government received a grade of C minus in network safety and that the Department of Defense and the Nuclear Regulatory Commission received failing grades under standards set in the Federal Information Security Management Act.[12]

The vulnerability of the United States to information warfare is enough but when nuclear weapons and the possibility of future nuclear crises are factored in, the future becomes dangerous. There are two scenarios by which information warfare could greatly increase the chances and/or result in a nuclear war for the United States. The first scenario could occur during a crisis with another nuclear power. Information warfare tactics could be employed by a third party (such as another state or a terrorist

organization) or even the other nuclear power, to influence intelligence and create the belief that a nuclear attack is necessary. The secondly in the absence of a crisis situation, information warfare tactics could be employed to create or manufacture a conflict between nuclear powers and escalate.

The first scenario presents several problems for policy makers and military leaders, specifically with regard to any attempts to predict the behavior of potential adversaries. During times of crisis, a time crunch is already in effect for all decisions, straining a leader's ability to debate a full range of options. Infowar "can cause flawed images of each side's intentions and capabilities to be conveyed to each other, with potentially disastrous results."[13] For example, a third party could take down power and communications systems and spread false intelligence about an adversary. Imagine what would happen if during the Cuban missile crisis power systems, phone lines, and TV signals in the United States shut down and the Pacific Fleet started receiving instructions contrary to actual orders (from an outside source, see "Eligible Receiver") and communications between the United States and Soviet Union were cut off while media reports about an impending attack circulated. The possibility of war is greatly magnified and the likelihood of a falsely reported nuclear attack (called a Type II error) increases exponentially.[14]

Furthermore, the actor engaging in the infowar doesn't even have to be all that active: "Suppose one side plants a virus or worm in the other's communications networks. The virus or worm becomes activated during the crisis and destroys or alters information."[15] This breakdown of communication could also force a nation's hand when nuclear weapons are in play:

> False indicators planted by the other side's infowarriors to bring down air defense systems and missile attack warning radars are harbingers of disasters once forces and command systems have been alerted to war-expectant levels. Under those conditions, the vanishing of information from radar screens or fusion centers could be assumed as the first infowave of nuclear attack, calling forth a preemptive response.[16]

Also by changing the perceived balance of power, an infowar breaks down traditional forms of deterrence. Even during peacetime, infowarfare could manipulate intelligence and media reports to tip strategic perceptions of friends or enemies.[17] Imagine what false intelligence and media reports about military force movement or technological advances could do to perceptions. Furthermore, manipulation of media and intelligence during a crisis situation could greatly contribute to fears of an enemy first strike, wrecking deterrence doctrines and resulting in the outbreak of an accidental war.[18] This scenario is particularly relevant based on past Department of Defense projections.The past infiltration of US civilian public works systems and defense systems suggest mapping of the networks by outside actors for a possible decapitation attack in a time of conflict.[19] This means that in foreign war rooms most likely there are plans for shutting down American infrastructure if a conflict were to break out and some reports suggest that China has a plan to take down American systems in the event of an invasion of Taiwan.[20]

The second scenario for of the escalation of infowar into nuclear conflict could be maliciously or accidentally caused. Infowar strategies could start a conflict between nuclear powers or manipulate a nuclear power into accidentally launching nuclear weapons. As shown above, the ability of infowar to break down deterrence doctrines can also cause conflict when no crisis exists. Specifically, a third party could attempt to create animosity between the US and another nuclear power via manipulation of

intelligence and media reports. Once the tension is felt between the nations, the actor engaged in infowar could unleash a blitz to deny the US its command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) structures, leaving the US in the dark and creating panic.[21] Furthermore, if US ICBM or SLBM detectors were hacked into, false images could be created in US early warning systems of a potential enemy strike, forcing an immediate US response. Remarkably this could happen completely by accident: an enemy could miscalculate the effect of its infowar strategies on the US or could have a program malfunction resulting in global disaster.[22]

While the US is vulnerable to infowar strategies, it also has doctrines and technologies that would largely prevent an accidental nuclear war. During the Cold War and afterwards, the US employed an approach called "phenomenal redundancy" to prevent an accidental nuclear launch.[23] Phenomenal redundancy is a process where the nuclear alert systems are backed several times to make sure that the best information is received This means the US has multiple spy satellites monitoring potential launch sites, backed by other satellites that look for heat signatures from missiles, followed by a radar net across the US that would pick up missiles, and agents on the ground providing visual confirmation. All of these technologies seek to create a redundancy that ensures against misinformation.[24] If an agent of infowar penetrated one layer of the US' nuclear detection umbrella the correct information would filter through via any of the other channels .

The final possibility for concern is the American security umbrella and the threat of nuclear proliferation. For the purpose of this paper, one should assume the "nuclear

pessimist" position, that the spread of nuclear weapons is destabilizing and makes nuclear conflict more likely.[25] An infowar has the ability to change perceptions on the battle field and in states' strategic conflict planning, however, it has the ability to influence perceptions of protection, specifically the protection of the US security umbrella.[26] The exploited vulnerabilities of US defense networks during future conflicts could destroy the confidence of its allies relaying US forces, causing them to develop their own weapons and possibly nuclear weapons.[27] This means that if the US is perceived as vulnerable to information attacks, other countries under its protection, such as Japan, Germany, and South Korea, would develop their own militaries and might also develop nuclear weapons to counter regional security threats. Furthermore, the vulnerability of the US could be used by outside actors to challenge US battlefield superiority, or even to hold the US hostage by threatening to attack the network infrastructure, furthering the degradation of the security umbrella.[28]

Red Panic-- Russia's Aging Technology and Infowar

Russia used to be a superpower and it used to have the sophisticated systems of redundancy for monitoring ICBM and SLBM launches. Since the fall of the Soviet Union, many of the radar systems and early warning detectors have fallen into disrepair, making it more plausible for a nuclear weapons accident resulting in a nuclear war.[29] Past instances have shown, the possibility for an accident is magnified when no outside interference is needed to bring about a potential disaster. In 1995 Russian military mistook a scientific rocket launched in Norway for a missile attack. President Yeltsin's nuclear briefcase was activated for the first time as he consulted with advisers. It took

about eight minutes to confirm that the rocket was headed out to sea and posed no threat to Russia.[30]

This is not the only situation of concern involving Russian nuclear preparedness.

> Russian early warning systems are failing, with many nodes no longer operational; the nuclear suitcases assigned to Russian leaders are falling into disrepair; local utility managers have cut off power to Strategic Rocket Forces bases because commanders have failed to pay the electricity bills; and there have been reports that system malfunctions have caused parts of the Russian nuclear arsenal to spontaneously go into "combat mode."[31]

Any of these instances, combined with the infowar scenarios outlined in the section above, could mean disaster. Due to the decline in Russian intelligence gathering services, Russia is more vulnerable to intelligence and media manipulation that comes with an infowar. Russian systems are even more vulnerable to hackers than US systems and, without the modernization of command, control, and communication (C3) systems that the US has pursued, it is even more likely that an outside party could successfully manipulate the Russian government. Furthermore, Russia is lacking in allies in the information technology community and a lack of credibility after the aforementioned hacking of the Estonian system. Specially after NATO responded harshly to Russian pleas of innocence, and both NATO and Estonian officials claimed it was a "planned attack on this nation's modern infrastructure."[32]

Several Russian doctrines are reason for concern in the case of an infowar crisis. Due to Russia's weakened C3, intelligence gathering abilities, and military strength, it is more reliant on nuclear weapons as an equalizer and as weapons of first use.[33] When

this is compounded with an infowar's abilities to change crisis perceptions and break down traditional deterrence beliefs, it spells disaster. Furthermore, Russia stated its position on the use of nuclear weapons in cases of infowar "Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself."[34] The possibility of an accidental Russian nuclear launch is an at all-time high given its stated policy of first use in an infowar and the lack of safety and redundancy surrounding its nuclear C3 systems.

The Neighbor in Need- Pakistani Technological Vulnerability

The nuclear rubicon has been crossed.

-Robert Rehbein

After nuclear Pakistani and Indian nuelcear testing in 1998, former United States President Bill Clinton declared South Asia "the most dangerous place on earth." There are several factors that make Indian and Pakistani hostilities deadlier than their Cold War counterparts: India and Pakistan share a common and disputed border, suffer from political instability, and the capitols can be reached in less than five minutes by missile. This makes the situation akin to a prolonged Cuban Missile Crisis bringing a permanent crisis atmosphere.[35]

Besides the close proximity of a hostile rival, other issues are alarming about Pakistan's nuclear arsenal. For example, US officials believe that during the 1990 war over Kashmir, the Pakistani prime minister, Benazir Bhutto, was cut out of the decision making process for nuclear release by military leaders who had begun deploying

nuclear weapons on fighter aircraft.[36] Moreover, Pakistani nuclear weapons lack the strict control features found on US and Russian nuclear weapons, specifically the two-man rule --requires that two vetted individuals consent for movement, launch, and detonation--, permissive action links--electronic locks preventing detonation unless the proper code has been entered--, and environmental sensing devices--prevents a detonation unless certain delivery parameters are met--, each of which are crucial components to prevent accidental nuclear detonation.[37]

The core problems with Pakistan's nuclear arsenal are not limited to the weapons themselves, but are part of an overall gap in intelligence gathering capabilities. While Russia's early warning and radar systems are falling apart, Pakistan (and India for that matter) does not have these technologies at all, creating a much smaller margin for error during a crisis. Imagine the scenario presented above involving Russia and the weather rocket taking place in Pakistan. Considering that the capitols of India and Pakistan are only a five minute missile flight apart, the country's leadership doesn't have the eight minutes it took Russia to determine the rocket was not a threat. Under these high stress conditions and with the lack of C3 structures in Pakistan, the possibility for false information causing catastrophic results is real.

Pakistan is in a dangerous condition due not only to its lack of redundancy, but also to the lack of any verifiable warning system.[38] This makes it easy for a potential agent of information warfare to create panic conditions that would bring about accidental nuclear war. If a hacker were to break into Pakistani radar systems displaying a fighter group or a ballistic missile coming towards Islamabad, there would be no time to verify before a retaliation decision had to be made. Moreover, an actor

could manipulate Pakistani intelligence gathering and make it seem like Indian attack was on its way, putting the Pakistani leadership on high alert and sparking hostilities that could spiral into conflict. Finally, since the current Pakistani nuclear weapons storage policy during peacetime is to keep them separate from their launch vehicles, during a crisis time the weapons would be ready on launching vehicles, the possibility of theft would be raised.[39] An organization desiring nuclear weapons could use infowar strategies to create panic in Pakistan and then try to steal the weapons while they were being moved, creating disastrous possibilities.

Possibilities for the Future

> Our machines that function in this environment are like the early biplanes compared to the 747 or the B-2, and our mastery of this environment is akin to our mastery of the air in the 1920s.
>
> -Dan Kuehl

The situation surrounding information warfare and nuclear weapons is worrying and action is necessary. First and foremost, the US needs to aid the nuclear powers of South Asia by providing them with command and control technologies, specifically permissive action links and environmental sensing devices that would greatly increase the safety and security of India and Pakistan's nuclear weapons. This is especially important considering the fragile nature of the two governments and the fact that radical factions within both countries are actively pursuing nuclear weapons.[40]

Next, an international consensus should be reached regarding the use of infowar in times of conflict and peace. Either through new treaties or security arrangements, or via the creation of NGOs and IGOs to help monitor and report on malevolent occurrences in information traffic, a standard should be set regarding what can be allowed in terms of information manipulation.[41] This will both encourage openness regarding exchanges of information and also curry "info-relations" that can be used to solve future problems.[42]

Another option for international action is to transform traditional military measures to make them suitable for information strategies. For example, this could be done through information sharing (specifically with peer competitors like Russia or China) concerning information warfare capabilities and potential threats or carrying out confidence building measures and joint exercises with information technologies aimed to decrease tensions.[43]

In the US, the problem is finally being recognized but there is still much to be done. Due to the trend towards interconnectivity, important industries in the US are at risk, such as nuclear power plants, moving away from their proprietary and more secure networks to more common and less secure, open-standard networks.[44] Obviously, more security is needed. The US Department of Homeland Security has established the sub-department of cybersecurity and telecommunications to attempt to "reduce vulnerabilities so those attacks don't happen in the first place."[45] Furthermore, the US Air Force has set up a cyberwarfare group, called the Cyberspace Command, to aid in both the execution and defense of infowar. President Bush has also signed a secret directive that creates a doctrine for infowar, under which specific conditions must be

met for the US to attack an enemy computer network. Former Secretary of Defense, Donald Rumsfeld, later issued"Information Operations Roadmap" outlining the Defense Department's future plans for infowar. But the most important part of any strategy is its execution, and despite the establishment of protection plans from information attacks, the US government still failed to achieve its own goals for increasing protection of its systems in 2006.[46]

Conclusion

> Victory smiles upon those who anticipate changes in the character of war, not upon those who wait to adapt themselves after changes occur.
> -General Giulio Douhet

With the world slowly shrinking, the nations of the world can't hide from the specter of information war any longer. Americans are in a position to prevent the repetition of history: an arms race is coming, one not based on bombs or bullets but on technology and the ability to control it. The choice is simple: does the world repeat the past and start a new phase of cold and hot wars revolving around this technology, or do we try to break the tracks? The future, in the words of Arquilla and Ronfeldt, will either be an electronic "Pearl Harbor" or an information age "Manifest Destiny" and the path for the world will be soon set.

The shadow of nuclear weapons will always hang over information warfare and the link between the two will only strengthen over time. Thus, the future of information warfare must be planned and prepared for as it may very well determine the future of

humanity. The first question is do we blindly sit by ignoring the warning signs or do we bravely march into the future in the hope of a better and safer world?

---

[1] Echevarria, A. (1997). Dynamic Interdimensionality: A Revolution in Military Theory, [Electronic Version]. *Joint Forces Quarterly*. 35(2). p. 30
[2] Cimbala, S. (Summer 1999b). Nuclear Crisis Management and Information Warfare, [Electronic Version]. *Parameters*, 117-128. Retrieved November 5, 2007 from Google Scholar.
[3] Ibid.
[4] Arquilla, J. & Ronfeldt, D. (Eds.), (1997). *In Athena's Camp*. Santa Monica: RAND p. 33.
[5] Ibid, 24.
[6] Ibid, 33.
[7] Cilluffo, F., Pattak, P., & Salmoiraghi, G. (2000). Bad Guys and Good Stuff: When and Where will the Cyber Threats Converge. *DePaul Business Law Journal*. Retrieved November 1, 2007 from Lexis-Nexis
[8] McMillan, R. (2007). Is the U.S. at Risk From Cyberwarfare?. *PC World* 25(10), 53-54.
[9] Cyberwar for real?: It looks like a war, it acts like a war and maybe the devastating computer attack on Estonia was a war (2007, May 29) Houston Chronicle. Retrieved November 9, 2007 from EBSCO.
[10] Cilluffo, Pattak, & Salmoiraghi, 2000.
[11] Ibid.
[12] "Cyberwar for Real," 2007.
[13] Cimbala, 1999b.
[14] Ibid.
[15] Ibid.
[16] Cimbala, S. (Summer 1999a). Accidental/Inadvertent Nuclear War and Information Warfare, [Electronic Version]. *Armed Forces & Society*, 25(4), 653-675p. 668)
[17] (Cimbala, 1999a, p. 654.)
[18] Ibid, p. 657.
[19] Khalilzad, Z. (1999). Defense in a Wired World: Protection, Deterrence, and Prevention. In Z. Khalilzad & J. White (Eds.), *The Changing Role of Information in Warfare* (pp. 403-437). Santa Monica: RAND. p. 408.
[20] Ibid, p. 410.
[21] (Cimbala, 1999b.)
[22] (Cimbala, 1999b.)
[23] (Cimbala, 1999a, 659)
[24] (Cimbala, 1999a, p. 662).
[25] Rehbein, R. (Spring 2002). Managing Proliferation in South Asia: A Case for Assistance to Unsafe Nuclear Arsenals. *The Nonproliferation Review*, 92-111, p. 94
[26] Davis, L.E. (1999). Arms Control, Export Regimes, and Multilateral Cooperation. In Z. Khalilzad & J. White (Eds.), *The Changing Role of Information in Warfare* (pp. 361-377). Santa Monica: RAND p. 364.

[27] Ibid, p. 364.
[28] Khalilzad, p. 405.

[29] (Cimbala, 1999b).
[30] (Cimbala, 1999a, p. 662-663).
[31] (Cimbala, 1999a, p. 670).
[32] ("Cyberwar for Real," 2007).
[33] (Khalilzad, 1999, p. 418)
[34] (Cimbala, 1999b).
[35] (Rehbein, 2002, p. 94).
[36] (Cimbala, 1999b)
[37] (Rehbein, 2002, p. 97).
[38] (Rehbein, 2002, p. 96-97
[39](Rehbein, 2002, p. 97).
[40] (Rehbein, 2002, p. 94).

[41] (Arquilla & Ronfeldt, 1999, p. xi).
[42] (Arquilla & Ronfeldt, 1999, p. xi).
[43] (Davis, 1999, p. 376).
[44] (McMillan, 2007)
[45] (McMillan, 2007).
[46] (Cyberwar for Real," 2007)