Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The China Syndrome

On April 1, 2001 a Chinese fighter jet collided with a U.S. Navy EP-3 surveillance plane off China's coast, resulting in the death of a Chinese pilot and the detention of the Navy plane and its crew. As Chinese and American diplomats sparred in the political arena, an army of Chinese hackers launched attacks against American web sites in protest. Though estimates vary, the ensuing "Cyberwar" between U.S. and Chinese hackers ultimately affected some 1,100 American web sites and 1,600 Chinese sites.1

Copyright SANS Institute
Author Retains Full Rights

AD

The China Syndrome

Charles Bacon

GSEC Practical Version 1.2e
July 22, 2001

On April 1, 2001 a Chinese fighter jet collided with a U.S. Navy EP-3 surveillance plane off China's coast, resulting in the death of a Chinese pilot and the detention of the Navy plane and its crew. As Chinese and American diplomats sparred in the political arena, an army of Chinese hackers launched attacks against American web sites in protest. Though estimates vary, the ensuing "Cyberwar" between U.S. and Chinese hackers ultimately affected some 1,100 American web sites and 1,600 Chinese sites.[1]

Whether this rash of web site defacements fits the description of Information Warfare (IW) is questionable. According to Ivan K. Goldberg, M.D., Director of the Institute for the Advanced Study of Information Warfare (IASIW)[2]:

> *"Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries."*

Though these incidents were disruptive for those affected, they amount to little more than electronic graffiti perpetrated by the street gangs of the information highway. During a recent senate hearing, Sen. Robert Bennett (R-Utah) dismissed these "Script kiddies" and hacker groups as "nothing more than a nuisance". While the damage caused was limited, the scope of the attacks was quite extensive and apparently well organized. White House security officials asserted that there was no indication that the attacks were linked to the Chinese government. However, given that Internet access is so tightly controlled in China, there is good reason to believe that the government allowed the attacks to proceed.[3]

A Brief History of China's Strategy

The involvement of civilians as part of a massive IW attack has been advocated as part of China's IW strategy since at least 1996. In a paper titled "Information War: A New Form of People's War "[4], the author states the IW is not just the domain of the military, but that anyone who understands computers can become a "fighter". The author envisions a force of "hundreds of millions" of volunteers assaulting enemy computer systems through the Internet. There is little hope of the government raising a force of this size within China anytime soon. According to a report in Jane's Intelligence Review[5], as of 1997, there were a mere 200,000 Internet users in China. By June of 2001, the number of users had risen to 26.5 million,[6] still far short of the number envisioned in the 1996 article.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

It would appear that the threat from civilian hackers, even as part of a well organized attack, is limited. According to Lawrence Gershwin of the CIA's National Intelligence Council, "For the next 5 to 10 years or so, only nation states appear to have the discipline, commitment and resources to fully develop capabilities to attack critical infrastructures".[7]

While it is unclear whether the Chinese hackers involved in the most recent web site defacements were acting with the support or encouragement of their government, there is evidence that some hackers involved in attacks following the accidental bombing of the Chinese embassy in Belgrade in 1999 worked for Chinese embassies in some African and European countries.[1] If the government were directing the recent web site attacks, perhaps they should be viewed as a tool of propaganda. Defacing an enemies web sites may be the 21st century equivalent of dropping leaflets from the air.

What is very clear is that the Chinese government has been actively pursuing an Information Warfare program for quite a while. China has long understood the need to advance their Infowar capabilities, but just how far have they advanced? Is China capable of launching an effective attack against the U.S. today? Is the work to better protect key infrastructure advancing fast enough to avert catastrophe, or are we losing ground? To begin to answer these questions, we should look at how Chinese views and capabilities have progressed.

In "Information Warfare", translated from articles published in Liberation Army Daily in 1995, the authors claim that the computer will be the key weapon of the 21st century.[8] The importance of operations against the Command, Control, Communications and Intelligence (C3I) infrastructure was cited repeatedly.

The Chinese were obviously paying attention during the Gulf War where the effectiveness of "preparing the battlefield" prior to a ground assault was made apparent to the world.

In the Gulf War, most operations of this type employed "hard weapons" (bombs and missiles) or Electro-Magnetic Interference (EMI) to disable C3I targets. There is some speculation that Iraqi computer networks were also attacked, but there is little hard evidence to confirm the reports. If the U.S. military did engage in attacks of this sort, information about it is unlikely to be available to the public.

In "Information Warfare", the authors advocate the targeting of military computer systems using viruses, to help them achieve "information dominance". Simply stated, information dominance is "knowing all enemy information, while keeping the enemy from learning one's own". On a battlefield increasingly dependent on information technology, the importance of defending one's own infrastructure cannot be understated.

In another Chinese paper published in 1995, Major General Wang Pufeng restates the importance of information control and the need for China's military to adapt to the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

realities of IW. He asserts that IW is ultimately about people and stressed the need to develop university curricula to train people for IW and to engage government research facilities in advancing IW technology.[9]

"Unrestricted Warfare," a book published in China in February 1999, is a clear departure from previous writings on IW. Up to this point, there was little mention of civilian infrastructure as targets of IW. Written by a pair of Chinese Air Force officers, it proposes tactics for developing countries, in particular China, to compensate for their military inferiority vis-à-vis technically advanced adversaries such as the United States, during a high-tech war. In the book, the authors advocate a multi-faceted attack strategy. Civilian and military information systems are key targets. The objective of which is that "…the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis." [10]

While many of the strategies proposed in this book seem a radical departure from previous warfare practices, some of the ideas go back as far as ancient China. Sun Tzu on the Art of War[11] is known as "*The Oldest Military Treatise in the World".* Even though it dates back to around 500 B.C., the ideas it contains are still applied today. While the battlefield of today is far different than it was 2500 years ago, the tactics employed are very similar.

Control of information is the key objective of IW. Information has always been a major factor in the outcome of war. Tzu knew this to be true long ago, but it is even more critical today.

> *If you know the enemy and know yourself, your victory will not stand in doubt…*[11]

There are many ideas and strategies from Tzu that appear to form the foundation for China's IW strategy. One thing that stands out in Tzu and several of the writings cited above is the willingness to target civilian infrastructure as a means to achieve victory. Consider the following passages from Tzu in relation to the strategies described in "Unrestricted Warfare":

> *. . . to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting.*[11]
>
> *When fire breaks out inside to enemy's camp, respond at once with an attack from without.*[11]

Apparently, some strategies are timeless.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Rules of War

Several of the papers cited above put forth the idea of a "people's war", wherein a large contingent of civilian computer users are employed to mount massive IW attacks against the enemies of the state. While this is becoming more and more conceivable, it cannot be implemented without violating some of the most basic rules of conduct. The rules of war include specific guidelines regarding who shall be considered a combatant.[12] Hordes of civilian hackers sitting at computers all over the globe do not fit the strict description. As such, are these participants bound by the same rules and customs of war that apply to combatants, or are they free to use whatever tactics they chose? Perhaps, but if they are not combatants under the command of a superior, they are individually responsible any criminal acts. Apparently this isn't an area of concern for those who advocate for a "people's war". However, in addition to the IW programs of the regular army, China has begun to develop IW regiments within its reserve forces and has established a reserve IW training base through the People's Armed Defense Department.[15]

As China, and other countries pursuing IW programs advance their computer attack capabilities to target the financial systems, electrical utilities, water systems, and other critical infrastructure through the computer networks that control them, they increasingly risk running afoul of international treaties the govern the rules of war. Attacks that specifically target military infrastructure (a power system or communication facility dedicated to military use, for example) are acceptable. However, if both civilians and the military use those systems, they should be considered "off limits".

A 1999 article written by William Church, Managing Director of the Centre for Infrastructural Warfare Studies, cites numerous examples of the problems with IW as it relates to the rules of war.[13] Numerous international treaties, beginning as early as 1863, have been established to help protect civilians from becoming unnecessary victims of war. The most recent, and most applicable, are the Protocol I additions to the 4th Geneva Convention of 1949, which were put into force in 1977. Protocol I has been ratified by 138 nations, including nearly all NATO countries, Russia, China, but not the United States.

While Protocol I does not specifically address IW, several provisions of it can be interpreted to include IW attacks. In "Unrestricted Warfare", the authors suggest disabling financial, electrical, communication and media networks as a means to create chaos in the civilian population. This would be a clear violation of Article 54 of Protocol I, which states:

> *It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the*

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

motive, whether in order to starve out civilians, to cause them to move away, or for any other motive.[14]

While this article is not specific to attacks on computer systems, any attack that had the result of shutting down civilian electrical distribution systems, water systems and the like would ultimately result in depriving the civilian population of sustenance.

Further compliance problems appear with Article 57 of Protocol I when viewed in the light of Information Warfare. In his article, Church points out that IW weapons such as viruses and worms are difficult to control and should be banned under Article 57, Precautions in Attack, which states, in part:

> *Those who plan or decide upon an attack shall:*
>
> *(ii) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss or civilian life, injury to civilians and damage to civilian objects;*[13]

As weapons of IW, not only are viruses hard to direct, they are hard to stop once they have been released. Article 57 goes on to say:

> *An attack shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;*[13]

To be in compliance with this section, if a worm or virus released against a military target were to begin attacking civilian systems, it would need to be stopped. Given the increasing level of interconnection between civilian and government computer networks and the tendency for viruses and especially worms to propagate rapidly, canceling an attack is nearly impossible. This further enforces the argument that they should be banned.

China has been very active in research on computer viruses as part of its IW program. According to an article in Jane's Intelligence Review[15], part of China's training curriculum for its IW program includes classes on virus attacks and counterattacks as well as tactics used to deploy such weapons.

Further evidence of this can be found it the government's requirements for anti-virus software vendors. According to a recent article in The Wall Street Journal[16], companies wanting to sell their anti-virus products in China are being required to provide samples of malicious software to the Ministry of Public Security. Over the last several years, several companies have handed over about 300 samples of the most common viruses found on the Internet. Despite repeated pressure from the Chinese, companies have resisted handing over their complete collections of tens of thousands of malicious

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

programs from their research labs. The Ministry is requiring these samples under the premise of independently testing the anti-virus program's effectiveness prior to allowing sales to go forward. While this may be true, one has to assume that this will also assist the nation's IW program in developing new viruses for use against others.

If these programs put China in violation of treaties that they have ratified, why do they continue to push forward with the development of Information Warfare weapons and tactics? To find the answer, we need only look at the attitude of Senior Colonel Wang Xiangsui, one of the authors of "Unrestricted Warfare". In an extremely rare interview with a member of the Western press, he said, "We are a weak country, so do we need to fight according to your rules? No."

"War has rules, but those rules are set by the West," he continued. "But if you use those rules, then weak countries have no chance. But if you use nontraditional means to fight, like those employed by financiers to bring down financial systems, then you have a chance."[17]

Is China a Threat?

As we have seen time and time again, the computer systems that we depend upon for both civilian and military support are susceptible to attacks from many points. Case in point, the April attack and intrusion into a system of the California Independent System Operator, which oversees the states electrical distribution grid.[18] Report after report has been written over the last decade describing the problems and suggesting some remedies. The need to protect critical infrastructure that is largely privately owned and operated has resulted in the creation of the Critical Infrastructure Assurance Office (CIAO) in Washington, and the National Partnership for Critical Infrastructure Security (NPCIS), a joint effort between federal agencies and the private sector.[19] Both entities exist to promote the increased security of critical infrastructure and cooperation between the government and the private sector. Progress has been made, particularly in the financial, energy and telecommunications sectors.[20] There is still much work to be done. After all, security isn't a project; it's a process, one that will need to continue to evolve if we wish to be secure.

China lags behind the U.S. in the development of Information Warfare capability and will probably remain behind for some time. Lack of open access to the Internet and the need to control access to information resources will probably limit the speed at which they can progress, but their desire to advance should not be underestimated. China understands that it is in a position of weakness in this area, and feeling a bit frustrated and powerless against its more technically advanced rivals. Given this and the apparent vulnerability of some critical systems, we should be careful not to back the dragon into a corner.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[1] Hearn, Kelly, "Chinese hackers may be rallying forces", May 21, 2001.
URL: http://www.vny.com/cf/News/upidetail.cfm?QID=187706

[2] Goldberg ,Dr. Ivan "Institute for the Advanced Study of Information Warfare". URL: http://www.psycom.net/iwar.1.html

[3] "Chinese Hackers Elusive", United Press International, May 2, 2001
URL: http://www.newsmax.com/archives/articles/2001/5/1/220058.shtml

[4] Wei Jincheng, "Information War: A New Form of People's War", excerpted from Liberation Army Daily, June 1995.
URL: http://www.ndu.edu/inss/books/chinview/chinapt4.html

[5] Bristow, Damon, "Aisa – Grasping Information Warfare?", Jane's Intelligence Review, December 2000.
URL: http://www.infowar.com/MIL_C4I/00/mil_c4i_120100e_j.shtml

[6] "China shuts down nearly 2,000 Internet cafes: Xinhua", Yahoo! Hong Kong News, July 2001. URL:
http://english.hk.dailynews.yahoo.com/headlines/010720/technology/afp/article.html?s=hke/headlines/010720/technology/afp/China_shuts_down_nearly_2_000_Internet_cafes__Xinhua.html

[7] McCullagh, Declan, "U.S.: Fear Countries, Not Hackers", June 2001.
URL: http://www.wired.com/news/politics/0,1283,44742,00.html

[8] Wang Baocun and Li Fei, "Information Warfare", excerpted from Liberation Army Daily, June 1995. URL: http://www.ndu.edu/inss/books/chinview/chinapt4.html

[9] Wang Pufeng, Major General "The Challenge of Information Warfare", Chinese Views of Future Warfare, Edited by Michael Pillsbury, Institute for National Strategic Studies. Excerpted from China Military Science (Spring 1995).
URL: http://www.ndu.edu/inss/books/chinview/chinapt4.html

[10] Qiao Liang and Wang Xiangsui "Unrestricted Warfare", February 1999.
URL: http://www.terrorism.com/documents/unrestricted.pdf

[11] Sun Tzu, "The Art of War" (Originally written about 500 B.C.), Translated from Chinese by Lionel Giles, M.A. (1910).
URL: http://www2.norwich.edu/stuart/ww/artwar420.html

[12] "Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907." URL:
http://www.icrc.org/ihl.nsf/385ec082b509e76c41256739003e636d/1d1726425f6955aec125641e0038bfd6?OpenDocument

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[13] Church, William, "Information Operations Violates Protocol I", June 1999.
URL: http://www.infowar.com/info_ops/io_and_violations_of_protocol_i1.shtml

[14] "Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)", 8 June 1977.
URL:
http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079?OpenDocument

[15] Thomas, Tim, "China's Technology Stratagems", Jane's Intelligence Review, December 2000.
URL: http://www.infowar.com/MIL_C4I/00/mil_c4i_120100d_j.shtml

[16] Bridis, Ted, "China is Asking Software Firms to Provide Samples of Viruses", March 2001. URL: http://www.politechbot.com/p-01874.html

[17] Pomfret, John, "China Ponders New Rules Of 'Unrestricted War'", Washington Post Foreign Service, August 1999.
URL: http://www.infowar.com/class_3/99/class3_081699a_j.shtml

[18] Morain, Dan, "Hackers Victimize Cal-ISO", June 9, 2001.
URL: http://www.latimes.com/news/la-000047994jul010.story

[19] Verton, Dan and Hamblen, Matt, "Cyberattack report: Some progress made", Computerworld, December 2000.
URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO54691,00.html

[20] Radcliff, Deborah, "Could a cyberwar cripple the U.S.?", January 2001.
URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO56588,00.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced