Global Information Assurance Certification Paper

Selected Social Aspects of Psychological Operations In Information Warfare

Drew Brunson

"Communications without intelligence is noise;
intelligence without communications is irrelevant."
Gen. Alfred. M. Gray, USMC
http://www.airpower.maxwell.af.mil/airchronicles/battle/chp6.html

Perception is a phenomenon that the advertising industry has understood and capitalized on for a century. That industry understands that the way we perceive the people and the events surrounding us shapes our reality and influences our actions and reactions. Accepting that, we also accept that the manipulation of perception outside of the advertising world can have a profound impact on the real world. For example, in August of 1993 the United States formed a special task force under the command of the U.S. military to enter Somalia and capture Somali clan leader Mohammed Aideed in response to increasing attacks on U.N. forces in the country.[1] According to Martin Libicki, the Somalis killed 19 Rangers while Aideed lost 15 times that number, roughly a third of his strength. It was an undeniable defeat for the Somalis. But, when the pictures transmitted by CNN of cheering Somali soldiers dragging U.S. soldiers through the mud reached the States, public perception was affected, the will of the people for the continuation of the war evaporated and Aideed won the information war.[2]

And while there is evidence that Aideed understood other aspects of information warfare,[3] in this instance, he took advantage of the ability of global broadcasters to beam events directly into homes instantaneously with no regard to whether the events being broadcast were real or arranged.[4] Aideed created an action that sent a selected message to his foreign audience that strongly influenced its emotions and objective reasoning. In doing so, in managing perception in the U.S. citizens of events in Somalia, Aideed accomplished his objective.

In a human context, people tend to develop a sense of trust not only because we've been taught through our cultural experience to trust those around us, but also because of patterns we have seen repeated, such as the sun rising in the East. Trust also develops between individuals because there is a perceived benefit in cooperation.[5] When human capacity for trust is extended to computer systems, perception management has an opportunity to slip beneath the layer of trust and the ability to perceive deception.[6] Although perception management is a broad area, affecting efforts from altering the perception of truth to the security of specific operations,[7] this paper focuses on psychological operations; specifically, the exploitation of trust relationships to accomplish an attacker's objectives.

A reasonable question is "Why are we vulnerable?" In a report by the Defense Science Board Task Force on Information Warfare, written in 1996, the task force unequivocally lays the blame at our own doorsteps. "The reality is that the vulnerability of the Department of Defense – and of the nation – to offensive information warfare attack is largely a self-created problem. Program by program, economic sector by economic sector, we have based critical functions on inadequately protected telecomputing services. In aggregate, we have created a target-rich environment and the U.S. industry has sold globally much of the generic technology that can be

used to strike these targets."[8] From the standpoint of psychological operations, it's not so much exploited technology as it is that we have created a global information system we do not control and do not understand,[9] and this in turn creates additional targets for exploitation. Most recently, this problem is being exacerbated by the growing emergence of "always-on" connections being made to individual homes and small businesses.

As this is being written (June 2000) a news story has broken that a private security company has alerted the FBI that it has found a malicious program on some 2,000 computers that can be remotely activated to launch an attack on a site of choice – a Trojan. Many of these computers are privately owned and are on cable-modem or dsl always-on connections. In addition to the technological risk posed by the fact that many of these computers have very limited or no security, the users of these computers often are attractive targets for social engineering efforts for a simple reason. The very thought that they would be targeted for an attack is foreign to the owners. I have a coworker who recently purchased a 500 Mhz Pentium running Windows 98 with 20+ Gb of disk space and an always-on connection. He has it wired to his older system with a simple 10 Mb Ethernet connection and has file and print sharing on globally. Despite my advice, he has not installed any kind of firewall and uses both computers for things such as taxes, Internet buying and personal finance.

Many in the security community have been tracking the regular scans looking for machines open for a netbios connection. If my friend hasn't already been compromised by the scans to port 167, he almost certainly will be. Unfortunately, he trusts that his connection is being protected by his ISP in the same way that his office computer has been protected by my staff. He also doubts that he would be targeted because he's "just a little guy at home." The question becomes, what kind of social engineering would an attacker try to accomplish and what type of attacker would be interested in a target such as my friend?

From an information warfare perspective, there are three primary target audiences for the attacker using psychological operations – psyops. The attacker can focus on 1) the enemy, 2) those who are friendly to his cause, or 3) the neutrals; with each target chosen for a specific purpose.[10] In my friend's case, he would probably fall into the neutral category. So why hit him? If the attacker is simply a hacker/cracker/script-kiddie, it might be for nothing more than to grab a credit card number or prove to friends that he or she could do it. But, my friend is not an attractive target for those groups. It is difficult to imagine a cracker boasting, "Yeah, I broke into this guy's Windows 98 machine." Unfortunately, the dangers we face are not limited to those groups. We also face the threat of multinational efforts to subvert our defenses and find an economic, diplomatic or military advantage.[11] These efforts might be aimed not only at our defense structure, but also at our utility infrastructure, transportation, communications, finance and much more.[12] As Stephen Northcutt illustrated at the SANS Orlando 2000 conference, a target such as my friend could be used initially to identify his multiple points of contact to the Internet and then to isolate his networks through distributed denial of service attacks. We also cannot discount the potential entrance of organized crime into the equation, not to mention political activists and disgruntled employees.[13]

So, as more individuals – the neutrals – turn to the Internet to help them with tasks that have usually been served by personal service or other traditional means, tasks such as banking, tax filing, shopping, and personal communications, the Internet as a loci for commerce and

communication becomes increasingly critical both to the individual and to the business and industries that serve the individual. And while the commercial sector is beginning to realize the importance of security, the information on the virtually unprotected personal machines may very well hold the key to a crippling attack on any sector simply because those sectors exist to allow the personal machines to connect to do business.

From a psyops point of view, however, how is it done? In any attack, finding and exploiting a trust relationship can be a key to success for the attacker. Let's look at how a trust relationship can be exploited. One of the most often cited examples of a physical trust relationship that was exploited successfully is the Mitnick attack. Here Kevin Mitnick discovered a relationship between host A and host B. He was able to determine the probable response that host A would give to host B after receiving the initiating packet in a three-way handshake. He blocked host B with a Denial of Service attack and sent a packet to A crafted to look as if it came from B. He then sent the expected response along with a small payload that contaminated host A's .rhost file and caused host A at that point to completely trust Mitnick's computer. He dropped the attack on host B and simply accessed A as a trusted root user.

So, how might an attacker employ psyops against a trust relationship? One of the more common examples used to explain trust exploitation is that of the overworked call center. Imagine a worker at a large corporate call center. The caller has done some research and discovered that a new personal report has been hired by the CEO. He calls and identifies himself as Bill Wright who has just been hired by the boss. He tells him he's been working all day researching a project that the CEO wants a report on in the morning and he needs access to the system to put the report together. Unfortunately, he's forgotten his password and it's already 10 p.m. Can he get a new password or should he call the CEO and have him call? In a shop with strong security that would be an easy call, but it's easy to see that, in many cases, the call center worker would simply trust that the caller is who he says he is and give out a new password. The net result? The attacker gets in and can probably hide his tracks before the real Bill Wright complains.

If the company is also a prime contractor for the government, a public utility or even a company whose success or failure can severely impact the stock market, then the attacker has gained a tremendous advantage by simply manipulating information he or she has gained by infiltrating the system. But, let's go back to my friend.

Assume, for this scenario, that a group wanted to create a deleterious impact on the stock market. That group, perhaps over a period of months, maps IP ranges that are known to belong to public ISPs providing high-speed, always-on access to individuals and small-businesses and they map for the Netbios ports. As they map, a second team begins the infiltration process, finding those machines that are unprotected and that contain information, such as passwords to personal investment accounts, banking, etc. Even though these passwords may be encrypted, with modern cracking tools being what they are, at the end of the mapping period, they very well could have discovered thousands of accounts, including my friend's, that can be exploited. Choosing the time to strike, they simultaneously use these accounts to issue massive sell orders to the various brokers and close thousands of bank accounts with the money transferred to offshore accounts that they may, or may not, care about accessing. The distributed nature of this attack would make detection and prevention difficult, if not impossible, and would certainly sow

an atmosphere of fear and distrust that would severely affect the general economy.

Again, the question is why? Let us look at the three basic types of attack – strategic, consolidation and battlefield.[14] If the above scenario were executed by organized crime, it would probably fall into the battlefield type because they probably would be looking to cause a drop in stock market prices where they could step in and buy cheaply, thus allowing them to see an impressive gain as confidence rebounded. If a foreign government perpetrated the attack, it might very well fall into one of the other two categories. The attackers might be trying to distract the attention of the current administration away from what they might be attempting elsewhere (strategic) or attempting to bring together the economic resources needed to launch a more serious battlefield attack against us later (consolidation).

But, what is it that causes us, as a whole, to make it easy for those who would want to abuse that trust? In a culture where the phrase "trust is earned" is a familiar maxim, it would seem that we would be more eager to challenge than we are. However, trust also seems to be a social construct between two or more individuals. In both social and business milieu, as alluded to earlier, a need to trust develops out of the need to foster cooperation to achieve goals and objectives.[15]

If that is, in fact, the case, then how do we overcome this tendency and manage to protect our critical resources? Part of the difficulty we face here is that our focus tends to be on strengthening the security of our physical defenses, whether that be through encryption, perimeter-based defenses, host-based defenses or, preferably, a combination of the three. Unfortunately, we still have too few in system administrative positions who are security-aware enough to alter default installations on whatever machine they are setting up (whether it be Microsoft based or *nix based) to give an acceptable initial level of protection to their users. But, these are technological trust defenses and likely will always be open to attack.[16] And while hardening those physical defenses is undeniably important, I contend that what we often overlook is the most dangerous vulnerability – our users – and that is where we spend the least amount of time in education. Why do computer viruses such as the "I Love You" virus work? Because our users, whether corporate, governmental or private, haven't been taught how to protect themselves and change the paradigm of automatically trusting the email that announces it comes from Aunt Sue.

We must begin focusing on the end user and on those who provide connections to the end users. When virtually all private connections to the Internet were made over modems connecting to a DHCP server where each session was served with a different IP address, it was much less likely for a private machine to be compromised and efforts to compromise machines tended to be focused on commercial, governmental and educational systems. Today, however, that situation is rapidly changing and ISPs must accept the responsibility of advising or requiring their customers to install personal firewalls and give them the advice needed to properly configure and maintain those firewalls. They also must understand the need to properly filter their outgoing traffic to block and detect activity coming from within their networks that can be harmful to the general Internet community.

Educating the end user is going to be the most daunting task. The recent proliferation of email-related viruses has certainly helped to awaken many to the dangers, but there must be a

broader effort to educate and assist users in protecting themselves and us from the bad guys. To do this, the security community needs to do a better job in educating first the media and then the public through the media. Psyops can work both ways. As Northcutt and others have said, the difference between us and the bad guys is that we have permission – we have the intent to do what is right. So it is with perception management. We can manage perception so that people will realize the risks they actually face and take steps to protect themselves. In helping them to protect themselves, we also help to protect the rest of us on the Internet who could be attacked by their systems if they are compromised. Trust is wonderful when exercised in an environment where it is reasonable. In a global environment where criminals, unfriendly political forces and people who just don't care about others have the same rights and access as anyone, trust can be dangerous.

Education, not legislation, is the key component. Our government can pass all the laws it wishes, but it won't affect the traffic that is coming our of countries such as Korea, China and Singapore. We need to be communicating these messages with intelligence. That's why I chose the quote to begin this paper. If we know what needs to be done and don't communicate it effectively, then whatever else we do is irrelevant. If we scattershot our communications without filtering them through an understanding of the message we need to pass then all we are sending out is noise.

[1] http://www.ranger.org/somalia/somalia.htm June, 2000

[2] Libicki, Martin, "What is Information Warfare?" National Defense University, ACIS Paper 3 August 1995, http://www.ndu.edu/inss/actpubs/act003/a003ch06.html June, 2000

[3] Ibid

[4] Ibid

[5] Abrams, Steve, "On the Origin of Trust and Its Impact on Technology," Georgetown Essays On Information Warfare, Feb. 16, 1999, http://www.cs.georgetown.edu/~denning/infosec/iw-essays/v1n5.txt, June, 2000

[6] Ibid

[7] Report of the Defense Science Board Task Force on Operation Warfare – Defense, Appendix H, November 1996, http://cryptome.org/iwd.htm June, 2000

[8] Ibid, Section 2.1

[9] Ibid

[10] http://www.psycom.net/iwar.2.html June, 2000

[11] Op Cit, Report of the Defense Science Board Task Force on Operation Warfare – Defense, Section 2.1

[12] Ibid

[13] Ibid

[14] Op Cit, http://psycom.net/iwar.2.html

[15] Op Cit, Abrams

[16] Op Cit, Abrams