CYBERSPACE THE NEW WAR FRONTIER

Shaharudin Ismail and Zahri Hj Yunos
National ICT Security and Emergency Response Centre (NISER)
(This article was published in the STAR InTech on 21 June 2005)

Cyberspace is an ever-expanding global digital network which links many aspects of life, including business and communications.

While new technologies allow for enormous gains in efficiency, productivity and communications, they also create new threats from those who harbour bad intentions towards us.

The same infrastructure that we utilise to transmit information creates new opportunities for those engaging in cyberwar.

The cyberwar being waged today involves the exploitation of ICT (information and communications technology), which the adversaries might use as a new attacking platform.

This is because many computer systems in the world are interconnected through a public telecommunications infrastructure or the Internet.

In the article *Cyberwar and Netwar: New Modes, Old Concepts, of Conflict*, John J. Arquilla and David F. Ronfeldt refer to cyberwar as "disrupting or destroying information and communication systems and turning the balance of information and knowledge in one's favour, especially if the balance of forces is against one."[1]

Today, cyberspace is the new war frontier whenever there are conflicts between countries.

The popular method of a cyberattack is the defacement of websites. Web defacement is a malicious activity in which a website is "vandalised."

Often the hacker replaces the site's content with a specific political or social message. The hacker might even erase all the content from the site by relying on known security vulnerabilities to access the site's content.[2]

Below are some cases of cyberwar as reported in the media.

China-Taiwan

During the Taiwanese presidential elections in August and September 1999, pro-Chinese hackers acted against Taiwan.

They compromised about 165 Taiwanese websites, mainly defacing them, over the two-month period.

Their ultimate goal was to negatively affect and bring down Taiwan's infrastructure.[3]

Among the targeted sites were those of electricity, economic institutions, telecommunications and air-traffic control.

India-Pakistan

India and Pakistan have in the past engaged in cyber protest in disputes involving national and ethnic differences.[3]

After a cease-fire in the Kashmir Valley in 2000, hackers of both countries continued with hostile activities.

A group known as G-Force Pakistan was the most active hacker group claiming involvement in the cyberwar.

The pro-Pakistan hackers defaced more than 500 Indian websites, while only one Pakistani website was hacked into by the Indians.

United States-China

The United States and China have also been involved in cyberwar especially in 1999 and 2001.

These cyberwars typically occur after incidents of military conflict on the battlefield. The first cyberwar began after the United States accidentally bombed the Chinese Embassy in Belgrade, Yugoslavia, during the NATO (North Atlantic Treaty Organisation) air campaign in May 1999.[3]

Many of the US websites were defaced and massive e-mail campaigns were executed to gain sympathy and support for China.

For example, the US Departments of Energy and the Interior, and the US National Park Service suffered website defacements.

The White House website was taken down for three days after it was continually mail-bombed.

The next cyberwar, which occurred in May 2001, resulted from an incident where a Chinese fighter was lost at sea after colliding with a US naval reconnaissance plane.[3]

It also coincided with the second anniversary of the Chinese Embassy bombing by the United States in Belgrade and the traditionally celebrated May Day and Youth Day in China.

The attacks were led by the Honkers Union of China (HUC) who defaced and crashed over 100 websites, mainly government and commercial sites.

The Chinese hackers posted pictures of the dead Chinese pilot Wang Wei with profane messages calling for the downfall of the United States.

Pro-United States hackers responded with similar defacements to over 300 Chinese websites.

Palestine-Israel

The cyberwar between the Israeli and Palestinian hackers began five years ago when the prolonged peace talks between the two countries broke down.

In 2000, about 40 Israeli websites and at least 15 Palestinian sites suffered defacements at the hands of hackers.[3]

The Israeli hackers performed denial-of-service (DoS) attacks on websites belonging to the Palestinians.

The pro-Palestinian hackers hit Israeli websites and posted messages such as "Free Palestine" or "Free Kashmir."

In this cyberwar, it was reported that the pro-Palestinian hackers got help from the G-Force Pakistan hackers.

During this time, several US websites were also hacked into by the pro-Palestinian hackers. The hackers took down a lobbyist group's website, posting online group membership information and credit card numbers.

Japan-South Korea

During the first week of April 2001, pro-South Korean hackers attacked Japanese organisations responsible for the approval of a new history textbook.[3]

The textbook allegedly glossed over actions committed by the Japanese Forces during World War II.

The perceived reluctance of Japan to accept responsibility for its actions during World War II triggered anger from the South Koreans.

It was reported that a majority of the hackers were South Korean University students. The students crashed several websites, including those belonging to Japan's Education Ministry, Liberal Democratic Party and the publishing company responsible for the textbook.

Japan-China

In early August 2001, pro-Chinese hackers targeted Japanese websites after Japan's Prime Minister visited a controversial war memorial, the Yasukuni Shrine.[3]

In a short period of time, Chinese hackers defaced several websites belonging to Japanese companies and research institutions.

Tensions have been rising again between Japan and China this year when the Japanese Government announced that its companies would have the right to drill for oil and gas in a disputed area of the East China Sea.[3]

The situation worsened in April after the Japanese Government approved a history textbook that China says whitewashes Japan's wartime record during World War II.

Several Japanese government websites experienced problems where access to the affected homepage was hindered. It was reported that a Chinese website had urged Internet users to flood Japanese servers with irrelevant data.

Malaysia-Indonesia

A maritime territorial dispute in the Sulawesi Sea between Malaysia and Indonesia had moved into cyberspace in March as Indonesian hackers launched cyberattacks on Malaysian websites.

Many of the websites affected, including several government department websites, were defaced with hate messages against the Government of Malaysia.

MyCERT (www.mycert.org.my) reported that 256 Malaysian websites were hacked into in the first quarter of 2005, compared with only 42 in the preceding quarter.[4]

Conclusion

The impact of web defacements is great. It not only affects a country's security, but also its economy and culture.

Hackers can replace the information on websites with controversial content. They can even take full control of these websites and manipulate the information.

Hence, there is no longer integrity and confidentiality of information. If such cyberattacks become more rampant, Internet users could lose their trust in the Internet as a platform for online business especially when it comes to transactions using credit cards.

Hackers could also place inappropriate pictures on affected websites. This could embarrass the owners of the websites especially if the site belongs to the government or any highly-reputable organisation.

Web administrators must take full responsibility to protect their systems from cyberattacks. They need to patch their systems regularly in order to avoid vulnerabilities from being exploited by hackers.

Web administrators must also play an active role in ensuring that they are familiar with the latest trends and security issues in order to protect their systems from cyber attacks.

References

[1] Arquilla, J.J. and Ronfeldt, D.F., Cyberwar and Netwar: New Modes, Old Concepts, of Conflict, http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/cyberwar.html

[2] What is defacement? http://www.webopedia.com/TERM/D/defacement.html

[3] CyberWar, http://www.cybertelecom.org/security/cyberwar.htm

[4] MyCERT Quarterly Summary Q1 2005, e-Security, NISER's Quarterly Bulletin, 14 Apr 2005.

ABOUT NISER

NISER (National ICT Security and Emergency Response Centre) is a technical agency formed by the National Information Technology Council (NITC) and started its operation in November 2000. NISER has been specifically tasked to support the nation's Information and Communications Technology (ICT) security and cyber defence initiatives to avert potential intrusions and unlawful cyber-actions that could threaten the nation's critical infrastructure. NISER current services and efforts include of Incident Response (MyCERT), Computer Forensic Services, Security Assurance and Security Management & Implementation.

For further details, please contact NISER at:

National ICT Security and

Emergency Response Centre (NISER)

MIMOS Berhad

Technology Park Malaysia

57000 Kuala Lumpur

Telephone: +60 3 8996 5000 (General) | +60 3 8996 1901 (Direct Line)

Facsimile: +60 3 8996 0827

Email : info@niser.org.my | Website : http://www.niser.org.my