Combating Cyber Terrorism: Countering Cyber Terrorist Advantages of Surprise and Anonymity

M. W. David, K. Sakurai

Cubic Corporation

Kyushu University
Faculty of Information Science and
Electrical Engineering

Abstract

The paper proposes ways to counter the Cyber Terrorist (CT) advantages of surprise and anonymity. It recommends the creation of a Cyberint Analysis Center to develop and evaluate methods to improve the ability to detect, identify and deter Cyber Terrorist attack. It also proposes ways to implement responsible, accountable and identifiable use of the Internet, and deny anonymity to the attackers.

1. INTRODUCTION

This paper takes the position that the mission of organizations dealing with information security is not only to protect, detect and react, but to also try to predict and prevent Cyber Terrorism (CT). It proposes how to counter two of the key terrorist advantages of surprise and anonymity. At the tactical level of specific attacks, it is almost impossible to design systemic strategies for identifying the immediate threat details of exactly where, when and how an attack will occur. However, at the operational level, how cyber terrorists plan to use information technology, automated tools and identify targets may be observable and to some extent, predictable [9]. We do not discuss the policy level, but several questions need to be addressed in that realm. Is there truly a need to have anonymous access to the Internet? Whose interests does anonymous access really serve? Do the potential threats outweigh the perceived value of anonymous Internet access? We suggest the price of freedom is not anonymity, but accountability. Unless individuals and governments can be held accountable, we lose recourse to the law. In order to protect the innocent, all communications must be subject to the rule of law, and this implies their originators must be accountable, hence not anonymous [Davenport, 2002]. To counter the CT advantage of surprise, we propose the establishment of a Cyber Intelligence (CYBERINT) Analysis Center. To counter the CT advantage of anonymity, we advocate and propose a methodology for and responsible, accountable and identifiable (RAI) access to the Internet. The primary mission and objectives of the CAC will be to enhance the capability to predict, prevent or deter an attack. The goal of RAI access to the Internet is to improve the capability of defining the "who" related to an attack.

2. The Cyber Intelligence (CYBERINT) Analysis Center (CAC)

2.1 Mission and Objectives

In the most simplistic terms, provide intelligence analysis and reporting that will help prevent a surprise CT attack. However, this is far from simple. Therefore, we will review some efforts related to cyber infrastructure protection to provide an understanding of the CAC's role.

The President's Commission on Critical Information Protection (PCCIP) in October 1997 identified the basic mission and objectives of something like the CAC in broad terms. The commission recommended a strategy for infrastructure protection through industry cooperation and information sharing, a broad program of awareness and education, reconsideration of laws related to infrastructure protection, a revised program of research and development and a national organization structure. The commission proposed seven elements within this national organization structure. The sixth element was an Information Sharing and Analysis Center [19].

Dorothy Denning envisioned the PCCIP's Information Sharing and Analysis Center (ISAC) as consisting of government and industry representatives working together to receive information from all sources, analyze it to draw conclusions about what is happening to the infrastructures, and appropriately informing government and private sector users. Dr. Denning foresaw the ISAC initially focusing on gathering strategic information about threats, vulnerabilities, practices and resources to enable

Proceedings of the17 th International Conference on Advanced Information Networking and Applications (AINA'03)
0-7695-1906-7/03 $17.00 © 2003 **IEEE**

effective analysis to better understand the cyber dimension of the infrastructure [8].

In their present form, ISACs are organized with the private sector in conjunction with the National Infrastructure Protection Center (NIPC). These ISACs are related to sectors like telecommunications, banking, water supply, energy, etc. However, according to Col. Tom Gibson, Joint Task Force for Computer Network Operations (JTFCNO), they are very closed communities. Most of the ISACs are private meetings to which one must be invited to attend. However, none of the information is repeatable outside the meeting unless it is sanitized [15].

A Carnegie Mellon University report looked at information sharing from the perspective of Cyber Intelligence (CYBERINT). The report defined the purpose of CYBERINT analysis as follows [22].

(1) Identify the need for action.
(2) Provide the insight and context for deciding among courses of action.
(3) Provide information on the effectiveness of pursuing the selected course of action.

Ross Anderson has suggested research into how to port techniques and experience from the world of electronic warfare (EW) to the Internet. A subset of EW is traffic analysis, which is a tool of the signal intelligence (SIGINT) community. Traffic analysis is looking at the number of messages by source and destination. This can give very valuable information, not just about imminent attack, but also about unit movements. However, traffic analysis really comes into its own when sifting through traffic on public networks, where its importance (both for national intelligence and police purposes) is difficult to understate [1]. We suggest part of the mission of the CAC should be to support the conduct of traffic analysis on the Internet. The objective should of course be protecting critical infrastructure from cyber attack.

We propose the main focus of the CAC be on CYBERINT. Intelligence should provide the essential elements of enemy information (EEEI): who, what, when, where, why and how. That is, who will attack what, at what time and place, for what purpose and objective, and with what type of resources and methods. We believe the CAC's mission and objectives should be to identify these EEEI and those envisioned by Denning and Shimeall as stated above. The CAC's focus should be on fusing information from multiple sources to learn and analyze the tools, tactics and motives of the CT community, and the malicious hackers they must be distinguished from, or associated with. The analysis should have the objective of providing early warning or indications of a cyber attack. Efforts should be made to create databases and profiles/templates of attackers, and use them to distinguish a CT attack from the hacker or blackhat community attack. The CAC should not duplicate the mission and objectives of the various Computer Emergency Response Team (CERT) organizations, but utilize and complement CERT resources and capabilities. However, since the Cyber threat is a global one, which can come from anywhere at anytime, the mission of the CAC should include international information sharing, cooperation, coordination and recommended response where appropriate

2.2 Tools and Capabilities

We recommend the CAC should be a stand-alone entity with communications links to the front line defenders and response teams. Its primary mission, as noted above, will be the analysis and fusion of information from multiple commercial, academic and governmental sources. However, it should also have its own collection and data capture capability in the form of honeynets. The Honeynets should be a worldwide network of multiple systems, tied into and monitored on a 24x7 basis by the CAC. The Honeynets will provide the basis for learning more about the tools, tactics, techniques, and motives of the CT and blackhat threats [13]. While accumulating this data, the Honeynets can also provide the CAC with the ability to perform passive fingerprinting of the enemy side of Cyberspace. This passive fingerprinting is based on remote host signatures like time to live (TTL), window size, don't fragment (DF) bits and type of service (TOS) [12]. The objective is to help identify the actual source of the attacks.

The CAC will probably receive its largest volume of data from the worldwide CERT organizations. However, it should also be integrated with government related entities like the Strategic Command Space Command (SCSC), which may become the Cyber Space version of NORAD, the National Infrastructure Protection Center (NIPC), ISACs, the FBI's InfraGard program, Army CERT (ACERT), industry, academia and related global information security organizations. The CAC would use this data to try to supplement and refine the information already available from vulnerability databases at CERTs and commercial and university organizations offering monitoring, intrusion detection and vulnerability database support.

For example, the CERT/CC at Carnegie Mellon has issued a report on the development of an Incident Detection, Analysis and Response (IDAR) prototype, which may enhance the ability to collect data, structure and codify knowledge, and populate the software with the collected knowledge. The report states the IDAR tool is relatively complete, but the populating of the knowledge base is as yet not detailed enough to make IDAR

operational. Using the CAC as the central focal point for this knowledge base could provide a solution to this problem. Maintenance of the database is also a key operational issue. New tools, attacks and vulnerabilities are constantly being introduced, and these must be addressed [4]. Once again, the CAC could provide the resources and support to update and maintain the knowledge base. In return, the IDAR would facilitate an improved flow of data and information on incidents and attacks to the CAC's databases. The ideal situation would be for IDAR type of systems to be deployed at all critical infrastructure networks to assist in the early identification of an attack, and the attacker(s).

On the industry side, Fred Cohen & Associates have done mid-level depth studies of about 20 terrorist groups in recent years. They have developed an All.Net Security Database, which contains an ongoing record of causes/threats, attack and defense mechanisms, effects, and viewpoints on information protection. A key feature is cross-referencing to provide a linkage between the cause/threat and the mechanism or tool used by the attacker. It also cross-references defense mechanisms to indicate which defense might be effective under certain circumstances against the attack [6].

2.3 Proposed CAC Structure

Defining a complete organization is a difficult task. At this time we will only propose a generic, functional outline of the CAC. Actual staffing, manning, location, budget, etc. are the realm of policy and politics. Figure 1 is meant to provide a general framework of functions, organizations and communications to enable the CAC to accomplish its mission and objectives.

We have included the ACERT specifically because of its work with the US Army Land Information Warfare Activity (LIWA). LIWA operations include staffing of the ACERT. The ACERT maintains both automated and manual mechanisms for predetermining next-expected attacks from unauthorized or adversarial network intruders. The ACERT's predictive analysis methodology (PAM) is germane to any effort attempting to model future activities based on current exploitation of computer systems. Its success depends on consistent quality reporting from network system administrators and from Regional CERTs.

Analysis efforts include the following: triage, incident handling, relational, functional, and predictive analysis. Functional and predictive analysis support the development of indicator profiling, pattern analysis and intruder fingerprinting. These are key technologies, which are critical to prediction [18].

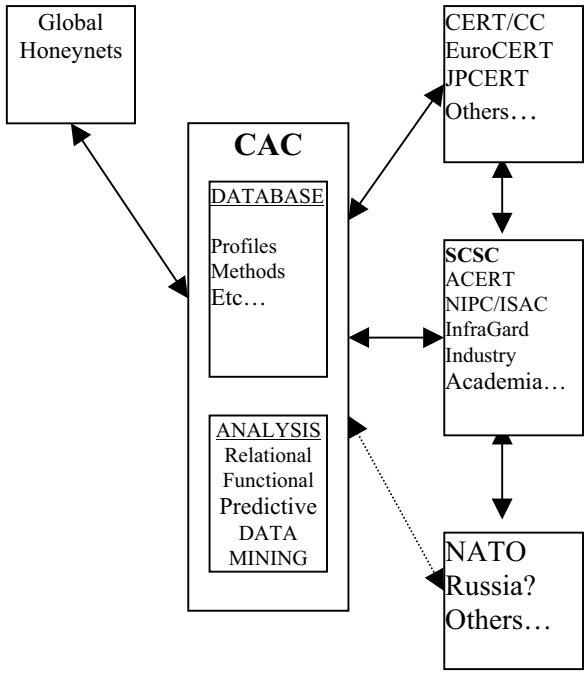

Figure 1. Generic outline of the proposed CYBERINT Analysis Center (CAC).

InfraGard is a government and private sector alliance. InfraGard was developed by the FBI in 1996 to promote protection of critical information systems. It provides formal and informal channels for the exchange of information about infrastructure threats and vulnerabilities [14].

The Business Software Alliance (BSA) has called for the creation of a Cyber Security Agency (CSA) within the proposed Department of Homeland Security (DHS). It points out strengthening cyber security requires analytical and technical capabilities that are related to, but also distinct from, traditional intelligence gathering and physical security functions. It states one of the chief missions of the CSA should be to ensure that the DHS, and the Federal Government as a whole, should acquire, deploy and manage technologies to protect sensitive information, and securely share that information [11].

Our proposal is for the analysts at the CAC to work as teams that concentrate on specific groups of critical infrastructure networks. It should have a real-live, warm-blooded human being available 7 x 24 x 365 capable of receiving, or issuing, some sort of an alert. We are living is a global village, so there has to be a real-time watch mechanism and a real-time communication mechanism [15]. The Critical Infrastructure Assurance Office (CIAO), NIPC and the Homeland Security Agency could specify the analytical sectors. However, an example of some of the teams could be as follows: air traffic control,

electrical power grids, water supply systems, dam control and emergency service networks [5].

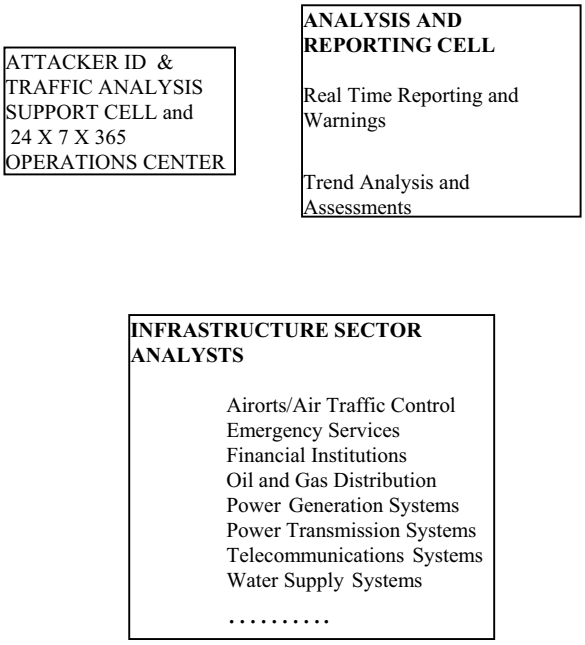

Figure 2. Functional Depiction of the CAC.

As with military traffic analysts in SIGINT, the teams would become familiar with the normal pattern of activity of the networks they support, and provide a human element of expertise in noticing deviations or anomalies that could indicate an attack was being planned, or was underway. They would also perform more detailed research and reporting based on data mining. Data mining would be conducted offline, and create knowledge or intelligence. The Data mining processes search for hidden patterns based on previously undetected intrusions to help develop new detection templates. In addition, data mining focuses on new hidden patterns in old data to create previously unknown knowledge or intelligence [3].

Data mining is a knowledge-creation process in which large sets of data are cleansed and transformed into organized and indexed sets of information. These sets of information are then analyzed to discover hidden and implicit but previously undefined patterns that reveal new understanding of general structure and relationships in the data of a domain under observation [24]. The CAC's analysts should become the experts in their sectors, and provide updated indicators, warnings and advice to the information security / assurance community. Depending on policy decisions, this could develop into a structure similar to the military advanced battlespace information system, which is designed to anticipate, deny or pre-empt an enemy attack [24]. That is, the CAC should eventually be integrated into an advanced cyberspace information system.

3 Responsible, Accountable, Identifiable (RAI) Access to the Internet

3.1 The Problem of Who

Dartmouth's ISTS issued a report titled "Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment". The report identified the greatest challenge facing cyber investigators as the area of log analysis. It also listed seven areas of concern, one of which was Internet protocol tracing. This is because Cyber attackers sometimes mask their identity to evade detection or use publicly accessible computers. The report goes on to say a combination of technological solutions and changes in public policy would help investigators trace an attack to its source [7]. Neils Johnson from Symantec notes, understanding where the bad guys are, what the bad guys are delivering and the kinds of things they are all doing is very, very important now, and will become even more important in the immediate, intermediate and long-term future [15]. In trying to accomplish this, anonymity is certainly a problem. Marc Goodman of INTERPOL has said, if we don't know who's doing what, it's hard for us to track the bad guys. We have to come up with the method of looking for a digital blood trail, and that's not particularly easy to do [15]. The essence of these observations and remarks indicates there is a need to identify who is using the Internet. From our perspective, this calls for responsible, accountable and identifiable (RAI) access to the Internet. Easy to say, but how to do it is a global policy and technical challenge. We will try to address some of the possible technical solutions to defining who, and dealing with anonymity.

3.2 Support of Network Forensic Analysis Tools (NFAT) and CAC

Computer forensics is a key technology that supports the identification of the source of incidents and attacks. Industry has come up with numerous tools to support the systems administrators and information security specialists involved in this activity. This paper is not meant to be a survey of these tools. However, there is a good overview provided in "Analyze This! – Network forensic analysis tools (NFATs) reveal insecurities, turn sysads into system detectives" [16]. The point is, there is a great deal of research and product development

underway to support the forensic identification process by using network-based intrusion detection systems (IDS). Putting these pieces in place is not hard; consolidating the data from disparate sources into one meaningful console is hard. This requires data fusion with an intuitive interface, and has not yet been accomplished. Another key capability that is needed is high-performance analyst interface [17].

Multisensor data fusion, or distributed sensing, is used to combine data from multiple and diverse sensors and sources in order to make inferences about events, activities and situations. Data-fusion technology has been applied to military applications such as battlefield surveillance and tactical situation assessment. Input into the cyberspace ID system would consist of sensor data, commands and a priori data from established databases. For example, system logs files, SNMP traps and queries, user profile databases, system messages, and operator commands. Output of the data fusion cyberspace ID system would be estimates of the identity (and possibly location) of an intruder, the intruder's activity, the observed threats, the attack rates, and an assessment of the severity of the cyber attack. Real-time human decision making processes would be supported by information derived from the fusion process. At the lowest level of interface, this would indicate the presence of an intruder or an attack. At the highest level the inference could be an analysis of the threat and vulnerability. The art and science of data fusion is directly applicable in cyberspace for intrusion and attack detection [3]. However, a proven system does not yet appear to exist.

3.3 Proposed System of Logical RAI Access

If a policy decision were made to require accountable, identifiable access to the Internet, one technical solution could be to require a registered token or smart card for logical access. A card like this would provide the basic token functions: authentication, verification, certification and encryption. Attached to it would be the identity of the individual. In countries where national identity (ID) card programs exist, this could be part of the information included in the multi-application ID card. In countries where they do not exist, it could be embedded in something like a driver's license or a bank automatic teller machine (ATM) card, which require verification of the holder's identity by the issuer. In a different approach, Mitsubishi Electric Corp. has developed a method that may provide every computer, every card and every semiconductor chip with an Artificial Fingerprint Device [23]. Reportedly, alteration and duplication are impossible, no additional cost is necessary, and its variation is large and randomness natural. Therefore, the accountability solution may be a combination of the Artificial Fingerprint Device and biometric tokens / smart cards for logical access onto the Internet.

The introduction and use of biometric tokens / smart cards as the basis for Internet access would make the job of identifying at least the computer from which an attack originates much easier. This loss of anonymity would hopefully limit the number of attacks by thrill seekers and so-called script kiddies, who would face possible legal action for their activities. Ideally, this would lead to a decrease in indiscriminate hacking, and allow information security specialists, government agencies and CAC analysts more time and resource to focus more malicious and dangerous threats to critical infrastructure networks.

Local logical access would be related to the personal, corporate or organizational public key infrastructure (PKI) being used in an individual and institutional environments. However, in order to accomplish fully integrated analysis and identification, there may be a need for a form of global PKI for international interoperability. This does not currently exist, and PKI implementers have found the development of technology outpaces the development of policy. Therefore, a global PKI is not likely to be achieved. One proposed solution is to incorporate a Bridge Certificate Authority (BCA) that users can decide to accept. The BCA model allows joined PKIs to select their own internal PKI model. As the global PKI develops it may be necessary to further expand the BCA into a structured mesh model [10]. This could provide a flexible solution where trust can be managed by end users. In this case the Global Internet Trust Register could provide an important end user service [2].

In any event, if the problem of anonymity is not addressed at its very source, the point of access, it will be near impossible to address from the top down. Therefore, anyone logging on to the Internet should have to do so by use of a registered and identified account linked to a token or some form of ID card.

4 Conclusions

Dr. Fred Cohen of Sandia National Laboratories has said "From the perspective of a security manager, cyber terrorism has not changed much about the way you operate, but it does produce some changes in the way you might want to respond to incidents. In particular, it should produce changes in the response processes and policies with regard to Internet use [6]."

All things being equal, the military defender has considerable advantage over the attacker. This is not true on the Internet. There, the attacker has the advantage. He can choose when and how to attack [20]. The fortress computer center or network was a good model when a

company or organization had its own unconnected networks. In today's world, where every network must be connected to the global network, it doesn't work as well [21].

Our CAC proposal is designed to help address the need for change in how we respond to incidents, and develop the capability to prevent surprise attacks. Our proposed RAI access system should be the focus of additional technical research and policy implementation on future Internet usage, with the objective of denying the cyber terrorists the ability to conduct anonymous attacks.

References

[1]Anderson, R.J.. Security Engineering – *A Guide to Building Dependable Distributed Systems*, Wiley 2001

[2]Anderson, R., Crispo, B., Lee, J., Manifavas, C., Matyas, V., Petitcolas, F. The Global Internet Trust Register, MIT Press, 1999.

[3] Bass, T. "Intrusion Detection Systems and Multisensor Data Fusion." *Communications of the ACM* Vol. 43, No. 4, April 2000, 99-105.

[4] Christie, A. The Incident Detection, Analysis, and Response (IDAR) Project. URL: http://www.cert.org/

[5] CIAO. URL: http://www.ciao.gov

[6] Cohen, F. Cohen Information Security Database. URL: http://all.net/CID/

[7] Dartmouth. Dartmouth Institute Examines Preparedness for Investigating Cyber Attacks. URL: http://www.dartmouth.edu/, 19 Jun 2002

[8] Denning, D. *Information Warfare and Security*. Addison Wesley Longman Inc., Reading, Ma. 1999

[9] Devost, M., Pollard, N. "Taking Cyber Terrorism Seriously – Failing to Adapt to Threats Could Have Dire Consequences." URL: http://www.terrorism.com, 27 Jun 2002

[10] Henderson, M., Coulter, R., Dawson, E., Okamoto, E. 'Modeling Trust Structures for Public Key Infrastructures. ' ACISP 2002, LNCS 2384, pp. 56 – 70, 2002. Springer-Verlag, Berlin Heidelberg (2002)

[11] Holleyman, R. BSA Letter to Chairman Tom Davis on Department of Homeland Security. URL: http://bsa.org/usa/press/newsreleases/2002-06-28.1185.phtml

[12] Honeynet Project. "Know Your Enemy: Passive Fingerprinting." URL: http://project.honeynet.org/papers/finger, 04 Mar 2002

[13] Honeynet Project. "Know Your Enemy: Honeynets." URL: http://project.honeynet.org/papers/honeynet/,11 May 2002

[14] InfraGard . Frequently Asked Questions. URL: http://www.infragard.net/faq.htm

[15] Kabay, M. "Information Security, Midyear 2002 Update: An Overview for Network Executives." URL: http://nww1.com/go/ad304.html

[16] King, N., Weiss, E. "Analyze This! – Network forensic analysis tools (NFATs) reveal insecurities, turn sysads into system detectives." URL: http://www.infosecuritymag.com/2002/feb/cover.shtml

[17] Northcutt, S., Novak, J. *Network Intrusion Detection – An Analyst's Handbook*, New Riders Publishing, Sep 2000

[[18] Northop Grumman. Land Information Warfare Activity.URL: http://www.northgrum.com/tech_cd/it/it_tasc_liwa.html

[19] PCCIP. "Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection" URL: http://www.pccip.gov, Oct 1997

[20] Schneier, B. "Natural Advantages of Defense: What Military History Can Teach Network Security, Part 1." URL: http://www.counterpane.com/crypto-gram-0104

[21] Schneier, B. "Defense Options: What Military History Can Teach Network Security, Part 2." URL: http://www.counterpane.com/crypto-gram-0205.html

[22] Shimeall, T. "Cyber Intelligence Analysis." URL: http://www.cert.org/archive/ppt/InterlDataExamp.ppt

[23] Vonderheid, E. "Artificial Fingerprint on a Chip Could Discourage Computer Crime", http://www.caffeine.ieee.org?INST/mar02/ffinger

[24] Waltz, E. (1998). *Information Warfare: Principles and Operations.* Norwood, MA: Artech House, 1998