Do We Really Know What’s Going On and Who the Enemy Is? Answer: Not Really.

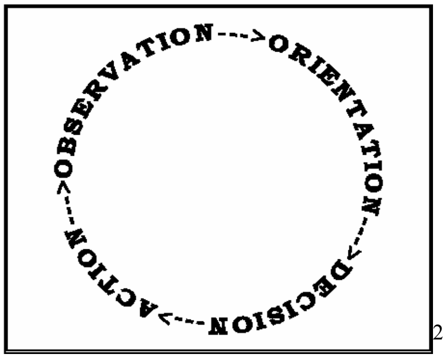
Abstract:

Success in combat is decided by which side makes better decisions faster. This process is commonly known as the Observation Orientation Decision Action (OODA)-loop. Since the decisions need to be made based on the observations of the environment and context in which the battle is taking place, the first two steps, Observation and Orientation, can also be described as Situational Awareness (SA) (i.e. “knowing what’s going on so you can figure out what do.”)[1]. The maintenance of the SA is hence of critical importance. The argument goes as follows: In order for us to truly be aware of our environment we must be first aware of what we have (Network SA) and where we operate (Strategic Context). The current technologies are not providing enough useful information to understand the complexities, and hence are not *aiding* in the creation and maintenance of Network SA. To improve this, a possible solution is introduced (Cyber Panel). This technology takes advantage of, not only event correlation but also the visualization of the threat to improve the understanding of what the attacker is going after (intent) and what are the interdependencies. The natural extension is that in order to making any inferences about intent, we must understand the enemy and the threat profile. The current methods of analyzing attackers are too simplistic and must be expanded to include variables that are not technical such as exogenous events and the decision making environment of the adversary (Strategic Context). Examples of such couplings are given. This in turn requires organizational changes. Lessons learned apply to both public and private sectors and while the language tends to be more military in nature, it is relatively simple to understand how the concepts and ideas in this paper could be extended to a private organization.

Introduction

Decision making in general is sometimes difficult, add stress to the mix and it may become practically impossible. Decision making while under attack is incredibly difficult indeed. While having clear and simple plans for dealing with contingencies eases the burden, sometimes the surprise of the attack does not leave time even for the plan. What commonly happens is that the defender is overwhelmed with the data flowing to him/her, leading to a paralysis as the decision maker’s decision-making cycle slows down. This cycle, commonly known as the OODA-loop, is of absolutely essential importance in times of stress. John Boyd first described the loop in his analysis of jet fighter combat and the decision making process that takes place in the cockpit. In fact, the entire act of combat is based on making better (more accurate and faster) decisions than your opponent and this is easier if one’s information flows are better than the opponent’s.

[1] See note 4.



[2]

- Observation: Data gathering from the surrounding environment.
- Orientation: Creation of a mental image of "…the circumstances in which the decision must be carried out."[3]
- Decision
- Action: The decision is implemented.

The goal of this model is to speed up the cycle, hence making decisions faster than the adversary. The decisions are made based on the situational awareness (SA)[4] perceived by the decision maker, which has been built as a result of historical knowledge, personal biases and the first two steps of the OODA-loop above. The better the operator's SA, the faster the decisions can be made. The systems that are feeding the loop and hence aiding in the generation of the SA are essential for the decision making to continue to be accurate and correct. The reason why this is relevant to defensive measures is that there currently exists a gap currently between the data and decision maker. This gap is the result of a reactive approach to security, which is obvious in the current state of detection mechanisms. The current state-of-the-art ID systems are pattern detection machines, essentially comparing past, known attack signatures or profiles to what is currently occurring. This type of analysis is susceptible to a problem similar to the human decision-making problem known as *availability bias*[5]. Availability bias is the result of a) misunderstanding the enemy, and b) "applying one's own culture onto the enemy"[6] translating into attack patterns that may be too narrowly defined and based entirely on the local 'hacking customs' or that the defender is expecting a certain type of an attack (i.e. a pre-scripted or known attack pattern). It is likely that the future generations of IDS applications will still be pattern matching, at least we should attempt to define possible patterns in advance and understand what those patterns mean to our systems. To this end Part 1 briefly discusses the current IDS systems and the current state of SA development and maintenance before moving on to discuss a possible future solution.

[2] Schechtman, p. 41
[3] *Ibid*, p. 42
[4] Let us first define what is meant by Situational Awareness: "… the perception of the elements in the environment within a volume of space and time, the comprehension of their meaning, the projection of their status into the near future, and the prediction of how various actions will affect the fulfillment of one's goals…" (Nofi, 9) or more simply "knowing what's going on so you can figure out what do." (Nofi,8)

[5] Gibb, p. 18
[6] *Ibid.*

PART I: The Current Network SA Development and Maintenance:

1) Know your Network

In the current network security setup, the creation and maintenance of network SA falls on the shoulders of the system admins, who need to create and run the scripts to pull together logs from a variety of sources, to watch out for alerts, to harden machines, etc. This activity does not leave much time for analyzing the data from the logs, even in the event of an intrusion. Even in the face of mountains of work, steps can be taken to at least create a baseline network model to use as a reference, i.e. audit the system.

It should be obvious that the application of this principle to the network security environment means that one must know one's own network, i.e. to understand what services/applications are running, what and who are connected to the network, and what is the current state of the defensive layers surrounding the network. To this end one can use network-scanning utilities like **nmap** to map the currently active machines and services.[7] This scan should be routinely run and compared to the baseline map to catch machine/service additions. One should also run utilities such as **cmp** on Unix from time to time to detect file replacements, even if no intrusion is suspected. The defensive system administrator should also include the scanning of BugTraq and other vulnerability listings and alerts services to enhance their SA. Log files from IDS systems, Firewalls, and Anti Virus systems should also be regularly scanned to understand the traffic in the network, even if no alerts have been noted. Obviously this is a time consuming task and not often done without a good reason.[8]

To alleviate the pain of this activity, the recent developments in cross-platform security management systems, such as netForensics' Active Envoy or E-Security's e-Sentinel, which collect data streams across platforms (firewall, IDS, router, etc) to a central security management console. These products are certainly a step in the right direction, but giving, say, IP address information is not necessarily useful since the IP address may have been spoofed to begin with. In essence, these systems give you an idea of where the intruders were, where they may have come from. Intelligent analysis is still needed to understand the reports and turn them into actionable information and this analysis, if made during a high-priority breach, demands more from the system, human and machine. Not surprisingly, intelligent attack analysis tops the wish list of a recent IDS users' poll[9].

So, some information is definitely missing in the current state about the attackers:

- Why are they here?
- What are they after?
- Who are they?

[7] See McColl, p 1

[8] For instance an OC-12 connection can generate over 800 Megabytes of event related data in an hour (Walker)

[9] Poll taken by Information Security Magazine, available online at: http://www.infosecuritymag.com/articles/august01/images/reader_poll.pdf

- Where are they?
- Given that system X has been corrupted by the attacker(s), what other systems are at risk and what are the mission critical components affected?

There are some developments in the drawing board to address these issues, and to a discussion about a possible future solution to this SA problem we turn to next

A Possible Future of Network SA management

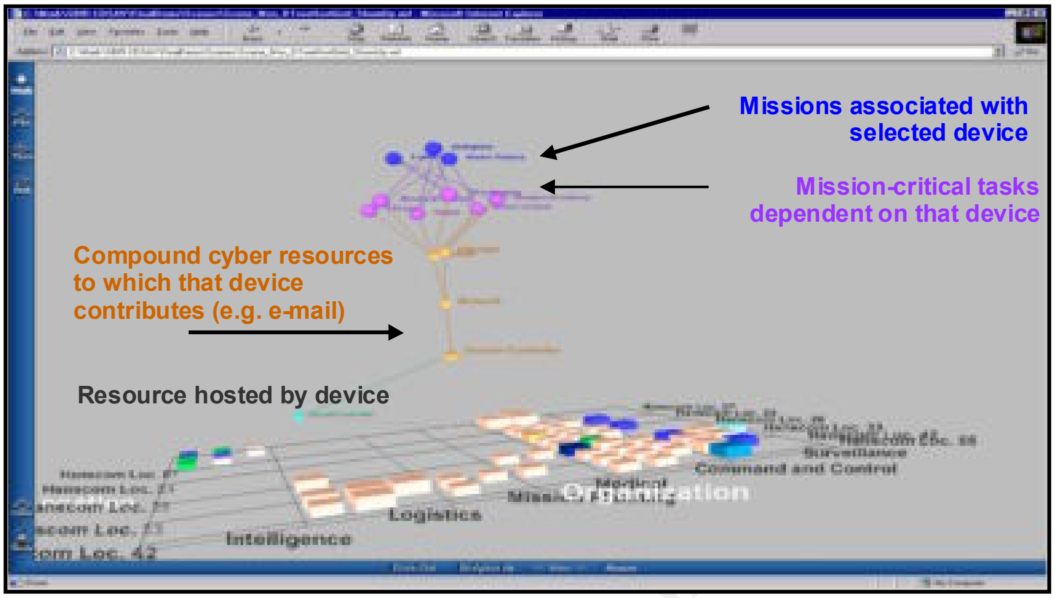
There is quite a bit of exciting research currently being done in the military field to improve network SA, including the Cyber Panel program[10] (a cross-platform SIM on steroids), the stated goal of which is

> "… to create and validate technologies that contribute to the ability to identify coordinated attacks, assess system health and mission-relevant attack effects, and choose and carry out effective security and survivability posture changes, either proactively or in response to the appearance of attacks. The technology products will include architectures and algorithms for multi-layered health sensing and attack detection, techniques for correlation across system layers and topology, models and techniques for attack tracking and impact assessment, analytical tools for generating and assessing security posture changes, tools and methods for dynamically reconfiguring security and survivability mechanisms, and attack model-based validation techniques. These technologies are components necessary for building an eventual advanced cyber defense system."[11]

What is of great importance to the person analyzing the breach is to understand the **time** dimension (i.e. frequency, temporal sequences, progress of the attack, etc.) as well as the **mission impact** (associations, and dependencies). Figure 1 shows the mission dependency screen of the prototype system, Figure 2 depicts the temporal (frequency) display.

[10] Other similar programs include SRI's Cyber Defense Research Center and Honeywell's SCYLLARUS intrusion situation awareness project.
[11] Objective from http://web-ext2.darpa.mil/ato/programs/cyberpanel.htm

Figure 1[12]

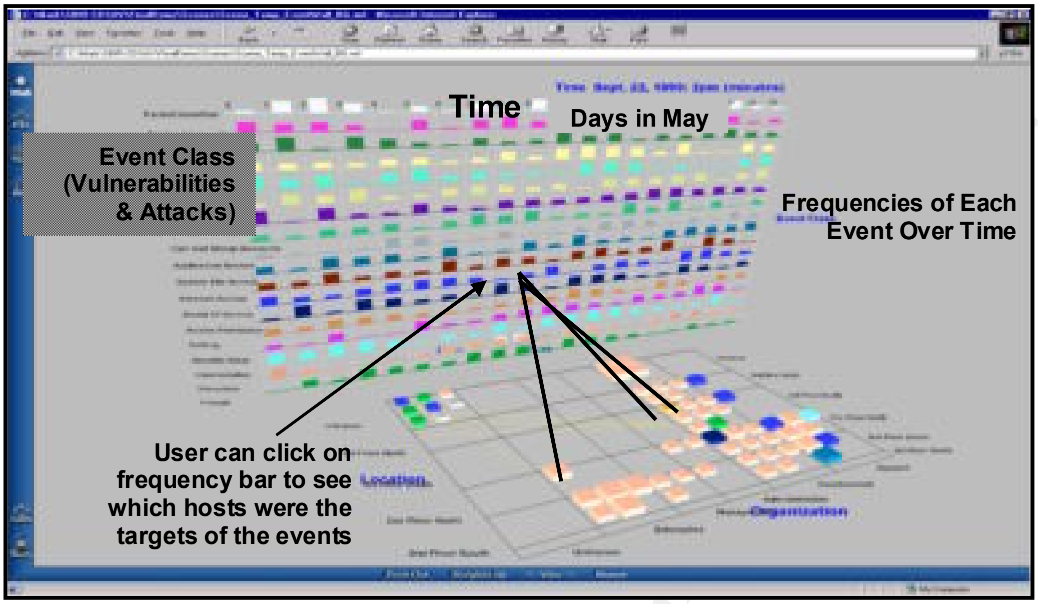

Missions associated with selected device
Mission-critical tasks dependent on that device
Compound cyber resources to which that device contributes (e.g. e-mail)
Resource hosted by device
Hanscom Loc. 27
Hanscom Loc. 21
Hanscom Loc. 22
Hanscom Loc. 23
Hanscom Loc. 42
Hanscom Loc. 55
Intelligence
Logistics
Medical
Mission
Organization
Command and Control
Surveillance

The purpose of the mission impact visualization is to show dependencies and relationships between the attack(s) and assets, as well as workarounds, e.g. if a mail server has been attacked, which assets can one substitute for it to still complete a critical mission (communication)? As can be seen, it directly enables enhanced decision making under stressful conditions through visualizations. According to CERT visual representation of data increases the usability of that data:

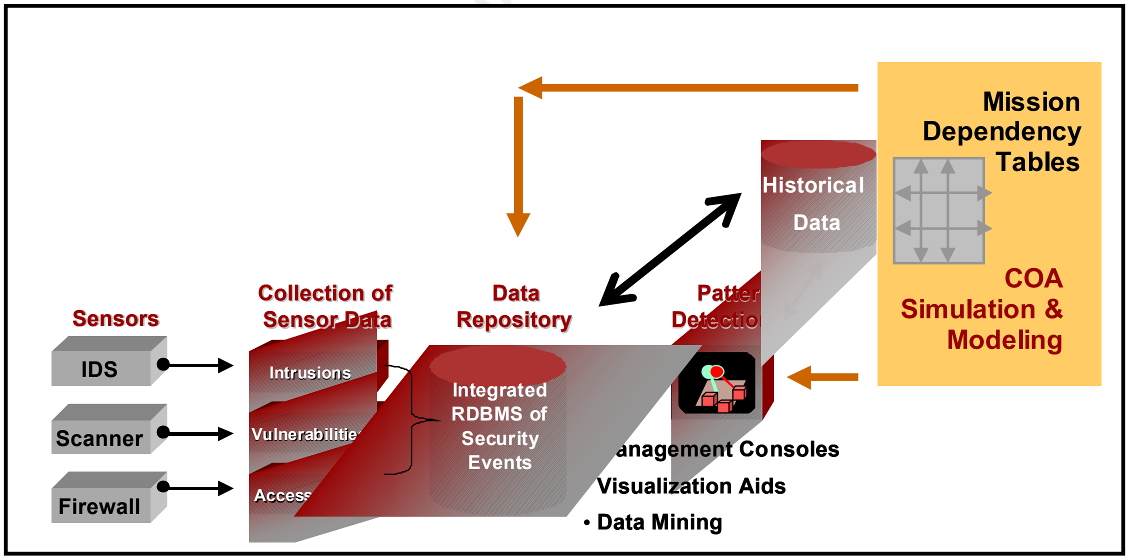
> "Ideally, however, people would be able to compute arbitrary functions on host and network data, to graphically view the functions using multiple visual formats, and to update the displays in real time so as to track events. Such capability could provide security managers with earlier warning indicators of an attack, provide additional assurance that machine diagnosis was accurate, and might provide insights indicating attacks of unknown types."[13]

[12] D'Amico, p. 26
[13] CERT, p. 90

Figure 2[14]


Time
Time: Sept. 22, 1999; 2pm (minutes)
Days in May
Event Class (Vulnerabilities & Attacks)
Frequencies of Each Event Over Time
User can click on frequency bar to see which hosts were the targets of the events
Location
Organization

The purpose of the temporal display is to present the analyst with the possibility of finding temporal patterns, including attack sources, targets, and network events to time. This is very important as it may expose previously unknown attack methods by, say, exposing that port 1234 followed by port 32819 led to entry through a previously unseen exploit.



The architecture of such a system is, in terms of the data gathering, similar to cross-platform security suite (such as netForensics) with the added bonus of using Course of Action (COA) and adversary modeling as a basis of creating attack patterns proactively. The way in which this process works is outlined in a model prepared by Zel

[14] *Ibid*. p. 14

Technologies[15] on the Intelligence Preparation of the Battlefield (IPB) methodology. This methodology is essentially a scenario planning and decision making tool. If the COA[16] simulation idea sounds familiar, it should, it is similar (at a rudimentary level) to penetration testing. COA takes advantage of using adversary modeling (using tools such as attack trees) and advanced Red Teams (such as DARPA's IDARPA team) to mimic the operations and mindset of a highly advanced adversary. The COA approach introduces the necessity to understand the enemy and his/her decision-making environment to increase our understanding of his/her capabilities.

2. Know Your Enemy: Adding Depth-of-Knowledge

Knowledge of one's enemy consists of knowing the enemy's methods, tactics, and motivations. We shouldn't stop there, however. These three generic categories give us absolutely no information about who and where the offender is, why they chose the system in question for attack (not all offenders are Script Kiddies), what the target within the system is (it the attack was targeted, maybe the offender is there for a specific reason), how they made the decision to attack in the first place, is somebody possible supporting this activity, the list goes on and on.

The current state of understanding the enemy is understandably weak and suffer from the serious problem that the US is one of the most technology dependent nations in the world, which in turn has led to security analysis being somewhat US centric. The steps already taken to gain an understanding of the enemy are the use of hacker profiling as well as the use of Honeypots to gather operational information on offender tools and methods. Both approaches have their shortcomings:

Hacker profiling suffers from the heterogeneity of the group and the lack of bona-fide profiles:

> "The security industry, law enforcement, and governments need to be extremely cautious not to generalize findings from the limited research to the entire hacker community. There is no generic profile of a hacker"[17]

This is not to say that profiling should not take place, rather that the operational history of computer offender profiling is simply not long enough.

Honey Pots suffer from the data bias produced by the most frequent type of an offender caught in the Pot, the Script Kiddie. While there is definite value in gathering this data in terms of tools and methods, the problem is that these interactions are typically the result of an automated attack launched against ANY target that will accept it. Chances are that since the more targeted attacks are, well, targeted, the pot will not be the 0-day target. This actually makes a good point for implementing Honeypots or other deception measures in most networks to capture information about the more targeted attacks, but I digress. The methods outlined above should be used but something else is needed to increase our understanding of the evolving offender field. The same way in which the application of the serial offender profiles developed in the US would probably not work

[15] This model is outlined online at http://projects.zeltech.com/ia/IPIB_FG/FG_Overview.htm

[16] The above model also outlines the use of COA.

[17] Rogers, p. 14.

in East-Africa (the offender is commonly a Caucasian male, between 25-35 years of age…)[18], the application of hacker profiles developed at any particular locale will not work globally. Additionally, the use of Red Teams that are simulating a more-highly advanced, well-funded, and highly-intelligent adversary. In order for this to be truly representative of the potential adversary, the team must understand what and whom they are modeling. Lessons could be drawn from the use of Navy or Air Force Aggressor Squadrons. These squadrons use total immersion to **become** the adversary.
This presents a dire need to expand the current method of thinking about the enemy to a much broader picture, to include a number of variables that are not currently (at least not seemingly) part of the analysis, namely:[19]

A. Culture: One must have an in-depth knowledge of the customs and history of the adversary.
B. Beliefs: One must understand the impact of societal beliefs and religion on the adversary.
C. Politics: What are the political views of the regime in charge and what is the level of political risk?
D. Economics: Understand economic interconnections, access to communications infrastructure, etc.
E. Military Doctrine: How does the adversary view Information Operations and Warfare.

The above variables form the adversary's decision-making environment which, given a problem, may yield wildly divergent interpretations precisely because the underlying assumptions are different. One of the main reasons why there is a need to include these variables is that the Western civilization makes up only about 20 percent of world's military manpower.[20] I.e. 80 percent of the military thought and doctrine is non-Western based. Further, according to a recent study by Predictive Systems, the majority of the non-US based attacks originated in South Korea, China, and Japan (collectively these three accounted for 73% of the tracked attacks in the study). Additionally, the use of the Internet is expanding outside of the US at a rate faster than within the US. This understanding of the potential adversary's decision-making environment is important, and especially so in the case of future adversary modeling and Red Teaming, as well as in the aftermath of an attack in understanding motives. The concept of availability bias mentioned earlier introduces serious errors and assumptions into the analysis of events, commonly leading one to think that the adversary's modes of behavior are somehow illogical and nonsensical:

> "The orientation of American leaders is different than the orientation of, say, Japanese or Chinese leaders. The orientation of capitalists and their leaders is different than the orientation of socialists and their leaders. Unlike knowledge systems, belief systems are highly individualized. Why? They include the stuff of the unconscious and

[18] Interestingly, the very usefulness of even serial offender profiling is now being questioned, see Sunde.

[19] This list is by no means exhaustive; rather it presents a base case.
[20] Huntington, p.88

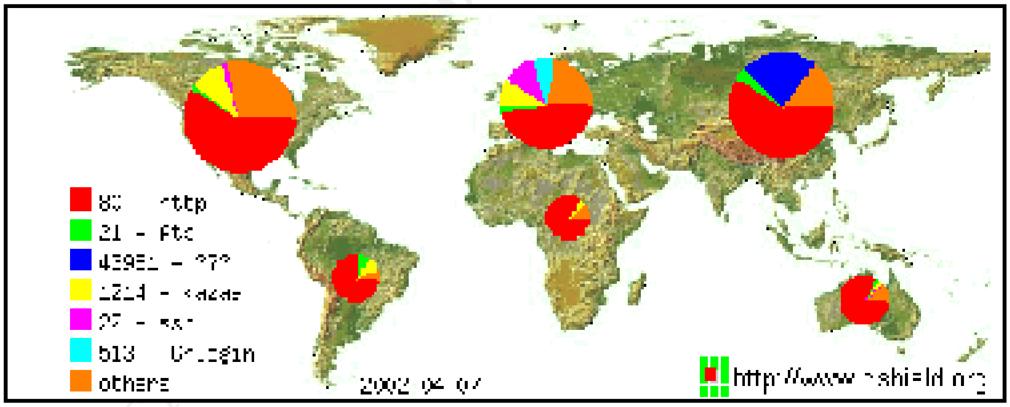
> subconscious, powerful elements of which others and even the bearer may be unaware."[21]

And further;

> "Thus the range of possible enemy intentions considered…must be considered within the cultural, political, military and doctrinal framework of the enemy society."[22]

The need gains an added sense of urgency once one introduces the notion of culturally variable views on information warfare. Consider, for instance, China; it has been well documented that its IW doctrinal development has embraced the concept of 'unlimited' warfare, essentially meaning that all targets, military or civilian, are fair game. To understand the severity of this threat, one only needs to consider how closely related the public and private sector are. A government contractor may have direct network connections to a government system for the sake of convenience. Attacking the contractor and then progressing to the government network is at the heart of this erasure of the target boundary. To take this concept to its absolute limit, one might even suggest the concentration on the so-called 'critical' infrastructure is somewhat of a misnomer since in a networked world EVERYTHING is critical with a few degrees of separation.

Some virtual organizations, such as the SANS Institute's Internet Storm Center, have taken on the task of analyzing incidents globally, but even with such organizations, the analysis on the purpose or intent of the incidents falls short. What is the reason, say, for the specifically Asian interest in port 43981 (the NetWare IP port)[23]?



Indeed it seems that the concept of *knowledge-in-depth* should be more closely examined, not only at the national level, but also in the individual organization context.

[21] *Ibid.* p. 44
[22] Cline, pgs. 14-15.

[23] http://www.incidents.org/

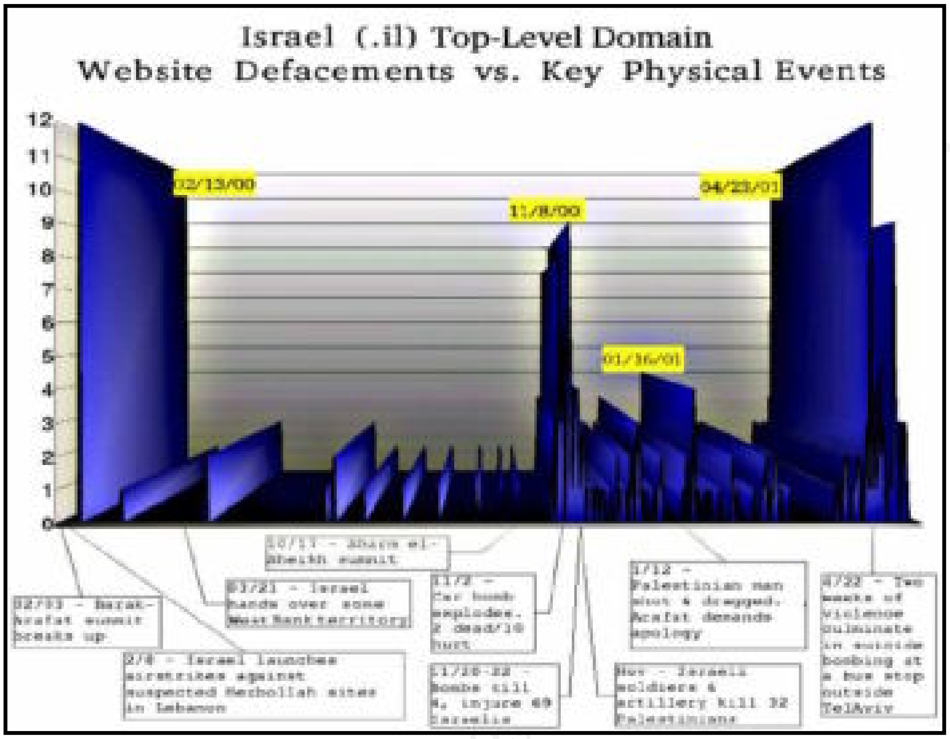
PART II. Strategic Context

In addition to the technological R&D in improving the network SA one must also consider the fact that ultimately the decision maker will (and should) be a human operator. To this end, an additional dimension needs to be added to the development of a 'holistic' view of the environment. This view must deal with the organizational side of INFOSEC, an addition or expansion of new capabilities to the analysis of threats and vulnerabilities. The SANS session on Information Warfare states that 'One thing that security professionals sometimes overlook is the study of fundamental networking and computing concepts.' I would contend that there is another, just as devastating oversight, namely the strategic context in which the network(s) operate. While having an understanding of your systems is essential, having an understanding of the world outside the network is critical. Let me give you an example of an intelligence technique that could be used as an early warning system: Company A that you work for is about to release a product that has been tested on animals. Do you think that there might be an increased likelihood of all types of protests, including electronic? If so, what steps should be taken to mitigate the risk of a virtual sit-in? How would you know that such a threat exists? You will not find that out from BugTraq or any other technical list. You will only know that if you know the context in which the organization you work for operates. Indeed, it has been argued by Shimeall et al. that

> "Historically, the more serious attacks will often have a specific catalyst: a corporation builds a production facility in a third world country that is viewed as an exploitive action by one or more activist groups; a government sponsors a peace conference that is viewed as an attempt to subvert the political viability of a disaffected part of the population; a repressive regime massacres a band of rebels near the capital; an organized crime syndicate reacts to crack downs by law enforcement."

Instances of this type of 'hacktivism' can be found in a number of incidents, ranging from the Israel – Palestine conflict to the accidental bombing of the Chinese embassy in Belgrade in 1999. Some evidence of such physical events triggering virtual events has also been presented by Vatis and is reproduced below in Figure X. He further concluded that:

1. Cyber attacks immediately accompany physical attacks
2. Cyber attacks are increasing in volume, sophistication, and coordination
3. Cyber attackers are attracted to high-value targets



While web site defacements may not amount to much more than harassment, the fact they are occurring at all, is akin to the Chinese concept of "People's War", the " …chance of the people taking the initiative and randomly participating in the war increased."[24], and, "…an IW victory will very likely be determined by which side can mobilize the most computer experts and part-time fans."[25]

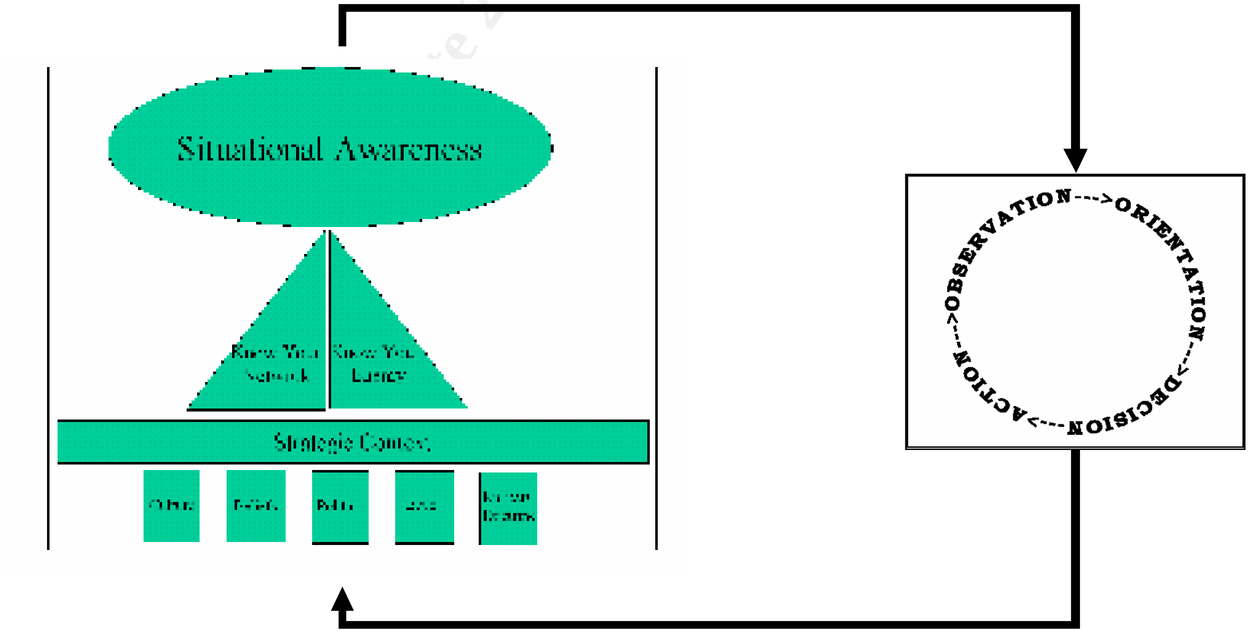
What this suggests as an additional defensive method is the cooperation of the (competitive) intelligence professionals within your organization must be debriefed on the existence of any exogenous threats. If your organization does not have such an arm, one should be established, even if that simply means that one of the System Admins begins doing rudimentary market research and analysis. This information can then also be used as method of deciding when own networks scans and audits should be run, given that the external threat environment points to an increased possibility of activity.

[24] Kleen, p. 4-4
[25] *Ibid.*

Conclusion

As shown above, the concept of Situational Awareness is of extreme importance, not only during a security incident, but also as a tool in predicting attacks and preparing for them in the event the prediction fails. The current state of network operational and tactical SA is left to the system administrators who are typically already overworked. The current IDS systems do not really support the systems administrators either, since the alert rate can be overwhelming and this is typically compounded by the amount and type of data combed from the various systems' logs. The more recent IDS systems have introduced the centralized security management console are a step in the absolutely right direction. We also caught a glimpse of the future in the Cyber Panel program, which is seeking to alleviate the data collection and analysis efforts and to enhance decision-making through visualizations of the network environment. Decision making ability is what makes a winner in a heat of battle, and currently the networks favor the offender, but only because the defender is obfuscated by the complexity of the interactions of all of the layers of the defenses. Once the defender can understand what is going on within the network, the offender loses the initiative. The application of more proactive attack pattern creation was briefly discussed through the use of Red Teams and adversary modeling and the use of COA analysis of the enemy's capabilities.

The future interconnectedness of the world also requires strategic measures to be taken to understand the correlations between physical and virtual events, the need for greater breadth in network defenses to include some relatively non-high-tech tools. While there are no guarantees and no single method is break-in proof, the fact that the human predictive analysis has been removed from the defensive posture to make room for all the technological whiz-bang solutions, is myopic.



The Iterative Security Knowledge-in-Depth Model

REFERENCES

1. Bass, Tim. " CC2 and Cyberspace Situational Awareness." www.silkroad.com/events/csspab3/docs/CSSPAB_CC2_Paper_V1.doc

2. Bass, Tim. "Intrusion Detection Systems and Multisensor Data Fusion." silkroad.com/papers/...acmp99bass.pdf

3. Belcher, Tim, Yoran, Elad, et al. "Riptech Internet Security Threat Report." http://www.riptech.com/pdfs/Security%20Threat%20Report.pdf

4. Cline, Donald L. II "Does the Theater Commander *Really* Know The Enemy: A Case For The Standing Theater 'Red Cell'" http://stinet.dtic.mil/cgi-bin/fulcrum_main.pl?database=ft_u2&searchid=101830710923537&keyfieldvalue=ADA378507&filename=%2Ffulcrum%2Fdata%2FTR_fulltext%2Fdoc%2FADA378507.pdf

5. Curts, Raymond J., Campbell Douglas E. "Avoiding information Overload Through the understanding of OODA Loops, A Cognitive Hierarchy and Object-Oriented Analysis and Design." http://www.belisarius.com/modern_business_strategy/campbell/ooda_and_objects.doc

6. D'Amico, Anita, Salas, Steven, "Visualizing Time Patterns and Mission Impact of Cyber Security Breaches" www.securedecisions.com/documents/DARPA2Summary.ppt

7. Daigle, Richard C. "An Analysis of the Computer and Network Attack Taxonomy." http://handle.dtic.mil/100.2/ADA391250

8. Frank, Diane. "DISA seeks detection system." http://www.fcw.com/fcw/articles/2002/0401/news-disa-04-01-02.asp

9. Garner, Karen T. "Situational Awareness: What is it? Can it be improved?" http://handle.dtic.mil/100.2/ADA307750

10. Goldman, Robert, P., Heimerdinger, Walter, Harp, Steven A., Geib, Christopher W., Thomas, Vicraj, and Carter, Robert L. "Information Modeling for Intrusion Report Aggregation." www.htc.honeywell.com/new/abstracts/idtp01010.htm

11. Huntington, Samuel P. The Clash of Civilizations and the Remaking of World Order. New York: Touchstone, 1999.

12. Hutchinson, Bob, and Skroch, Michael. “Lessons Learned Through Sandia’s Cyber Assessment Program.” www.naseo.org/committees/energydata/energyassurance/hutchinson.ppt

13. Kleen, Laura J., “Malicious Hackers: A Framework for Analysis and Case Study” http://handle.dtic.mil/100.2/ADA392952

14. Lunt, Teresa. “Intrusion Detection: New Directions.” http://cnscenter.future.co.kr/resource/rsc-center/presentation/black/vegas99/tutorial.ppt

15. National Infrastructure Protection Center. “ Cyber Protests: The Threat to U.S. Information Infrastructure.” http://www.nipc.gov/publications/nipcpub/cyberprotests.pdf

16. Nofi, Albert A., “Defining and Measuring Shared Situational Awareness.” www.cna.org/newsevents/images/crmd2895final.pdf

17. Parks, Raymond C., Duggan, David P. “ Principles of Cyber-Warfare.” http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperT2C1(10).pdf

18. Rogers, Marc. “Psychological Theories of Crime and ‘Hacking’.” http://citeseer.nj.nec.com/rd/40727521,380485,1,0.25,Download/http%3A%2F%2Fwww.escape.ca/%7Emkr/crime_doc.pdf

19. Schudel, Gregg, and Wood, Bradley. “Modeling Behavior of the Cyber-Terrorist.” http://www.rand.org/publications/CF/CF163/CF163.appc.pdf

20. Shimeall, Timothy J., Dunlevy, Casey J., and Williams, Phil “Intelligence Analysis for Internet Security” http://www.cert.org/archive/html/Analysis10a.html

21. Shimeall, Timothy J., Dunlevy, Casey J., and Williams, Phil. “Countering cyber war” http://www.cert.org/archive/pdf/counter_cyberwar.pdf

22. Shimeall, Timothy J., Dunlevy, Casey J., and Williams, Phil. “Intelligence Analysis for Internet Security: Ideas, Barriers and Possibilities” http://www.cert.org/archive/html/spie.html

23. Sidel, Scott. “Centralized Management. Command, Contain, Control.” http://www.infosecuritymag.com/articles/january02/features_command.shtml
24. Smith, Richard. “Country Threat. An Analysis of Internet Attacks.” http://www.predictive.com/pdf/Country_Threat.pdf

25. Spitzner, Lance, "Honeypots. Definitions and Value of Honeypots." http://www.securityfocus.com/cgi-bin/infocus.pl?id=1492

26. Steele, Robert David. " The New Craft of Intelligence: Personal, Public, & Political." http://www.intellnet.org/documents/1000/010/1017.doc

27. Sunde, Scott. "Ex-FBI Profiler: No such thing as a 'typical' serial killer." http://seattlepi.nwsource.com/local/54980_profilers18.shtml

28. Vatis, Michael A. "Cyber Attacks during the War on Terrorism: A Predictive Analysis." http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf

29. Walker, John Q. " Security Event Correlation: Where Are We Now?" http://www.netiq.com/downloads/Library/White_Papers/Security_Event_Correlation-Where_Are_We_Now.pdf

30. Walsh, Trudy. " Illinois data center posts virtual guard." http://www.gcn.com/21_3/tech-report/17858-1.html

31. Yoshihara, Toshi. "Chinese Information Warfare: A Phantom Menace or Emerging Threat?" http://carlisle-www.army.mil/usassi/ssipubs/pubs2001/chininfo/chininfo.pdf