



**Cs3 Inc.;**  
5777 W Century Blvd, Suite 1185  
Los Angeles, CA 90045  
Phone: (310) 337-3013  
Web: <http://www.cs3-inc.com>

## **Defending Government Network Infrastructure Against Distributed Denial of Service Attacks**

### **Table of Contents**

1. Distributed Denial of Service Attacks and Their Impact
2. Federal Network Security Initiatives and DDOS
3. Challenges of Building a DDoS Defense
4. How to Build a DDoS-Resistant Government Infrastructure
5. References
6. Appendix: Resources for Government Network Administrators

### **Section 1: Distributed Denial of Service Attacks and Their Impact**

Denial of Service (DoS) attacks are a class of network security threat whereby one or more attackers target network resources and servers to deny service to legitimate users. Increasingly, such attacks come from multiple, physically and network-topologically separated locations – a variation dubbed “Distributed” DoS attacks or DDoS attacks – making it harder to locate the attacker or thwart the attacker.

While people use the term “DDoS” rather broadly to include attacks that exploit bugs and vulnerabilities of programs, the term has gradually come to mean **packet flood attacks**. Packet flood attacks occur when the victim’s computing resources are overwhelmed by streams of bogus traffic from one or more attackers. To mount a successful DDoS flood attack, the attacker often establishes control over several unwitting “*zombie*” computers by hacking into them. Such compromised computers are then used in coordinated fashion to bombard the eventual victim with packet floods.

#### **1.1. How Serious is the DDoS Threat?**

It is believed that DDoS attacks have increased in frequency and severity. A recent study by researchers at the University of California, San Diego, conservatively estimates that there are more than 4000 attacks per week [1, 12]. The study illustrates that the threat of DDoS attacks is both real and imminent for any enterprise that relies upon the Internet to conduct useful, let alone mission-critical, business.

DdoS attack scripts have become quite common in the hacker community. Further, zombie infestation is spreading much more rapidly with the use of self-propagating worms like Code Red and NIMDA as occurred in July and September 2001. For a survey of readily available weapons to the attacker(s) see [18,19,20,21,22]. DDoS attacks are further made more effective by fundamental vulnerabilities in the Internet protocols that make it quite easy for attackers to falsify (or "spoof") the source addresses of the packets they send out.

*"Denial of Service attacks remain a serious threat to the users, organizations, and infrastructures of the Internet."* [19]

Kevin Houle, George Weaver  
CERT Coordination Center  
October 2001

A DDoS attack can be devastating in its impact on the intended victim. Financial losses from a DDoS attack can be very large (Yankee Group estimates that an outage of a few hours in 2000 at CNN, yahoo, eBay and others caused over \$1Billion in overall damages [9]). Attacks can also seriously disrupt all operations within the targeted organization. Grc.com was severely crippled by a so-called "script kiddie" [23] and there are even instances of ISPs having to shut down permanently thanks to such attacks [11,24].

Computer Emergency Response Team (CERT) [[www.cert.org](http://www.cert.org)], the Internet's venerable security sentinel and one of the agencies charged with studying and helping defend against denial of service attacks, has been warning that DDoS attacks pose a major threat to e-commerce and e-business.

## **1.2. Is the Government a Target?**

Like other visible and highly symbolic sites, the White House and other prominent Government sites have indeed been targeted by DdoS attackers [27]. Ironically, CERT was itself targeted for several days in June 2001 [25,26].

The Government is also concerned about DDoS attacks from other nation states that might target U.S. critical network assets in an "information warfare" scenario.

In a well-documented (unclassified) account [29], Colonel Gibson of the Joint Task Force/Central Networks Operations (JTF/CNO) told researchers at a DARPA meeting about a DDoS attack on the U.S. Pacific Command in April, 2001. The attack traffic had source addresses that were seemingly from the People's Republic of China, although the actual group responsible has yet to be identified. The attacks occurred in the aftermath of tense negotiations regarding the downed U.S. EP-3 earlier in the year. While none of the Command's internal networks were affected in the long-term, the ability of attackers to relatively easily disrupt critical Government operations that were reliant upon the Internet could never again be disputed.

*"The DoD is concerned about a concentrated nation-state attack. We have seen the harm done just by 'script kiddie' DDoS attacks on the DoD networks, and they are damaging enough. If someone got organized, they could significantly damage the infrastructure and the ability to get our military mission done. This isn't just a pipe dream for someone to do academic research on any more..."*

Dr. Douglas Maughan  
DARPA Program Manager  
Interview in March 2002

Experts from National Infrastructure Protection Center (NIPC) of the FBI have documented and studied patterns of cyber attacks and found that such attacks are increasingly complementing their terrorist counterparts in the physical world [14]. Howard Schmidt, who co-chairs the Critical Infrastructure Protection Board with the Bush administration's Cyberspace Security Advisor, Richard Clarke, described both the threat and the measures that the administration is contemplating to counteract the threat [16]. The questions that Schmidt's group is examining and their preliminary conclusions maybe found at [17].

## **Section 2: Federal Network Security Initiatives and DDOS**

Given the dimensions of the DDOS threat, it is useful to assess whether or not existing or currently planned Government initiatives have already taken this particular threat into account by addressing it in some fashion.

The traditional "CIA" concerns of security are: Confidentiality, Integrity, and Availability. Most tools and research efforts (whether Government-sponsored or not) have focused on these concerns largely from the perspective of the individual workstation. DDOS is a concern that spans several of these concerns, but from a network perspective. It turns out that little effort (both in terms of Government or commercial R&D) has focused on the "CIA" concerns from the perspective of the Internet. Perhaps, this is understandable because the emergence of the Internet for serious business is relatively recent. However, the "net" result is that the Internet is an uncommonly vulnerable public infrastructure upon which the Government and many of its critical operations rely to a degree unimaginable just a few years ago.

Figure 1 summarizes some of the major Government "information security" initiatives, and the degree to which they explicitly address DDOS as a problem. What the diagram demonstrates is that, while there are certainly visionaries within the Government now beginning to focus on this problem, there is nothing that is going to produce DDOS solutions quickly and in the short term. In general, however, the Government is aware of the threat at this point, and its initiatives in this area are still taking shape.

What Figure 1 illustrates, moreover, is that there is no currently planned Federal or centralized strategy to protect all Government infrastructures against DDOS attacks. The first initiative, GovNet, has stalled and most security and infrastructure technologists with credibility believe that it is the effort is fundamentally flawed in concept and can never be realized.

The Bush administration, through the Critical Infrastructure Protection Board, has just unveiled its "National Strategy to Secure Cyberspace." [36], a 65-page report that advocates an approach that shifts "from threat reduction to vulnerability elimination", which is a big step forward. The report forcefully argues that it wishes to promote a "national" (not "Federal") strategy for cybersecurity whose thrust largely comes from the private sector and not from the Government. In part, this is recognizing that even Government networks are connected to the Internet, and that, as with physical security, information security is a characteristic of the entire infrastructure, and not of isolated pockets. However, the report falls well short of proposing real solutions or details.

Name of Initiative	How it Deals with the DDoS Threat
Department of Defense Trusted Computer System Evaluation Criteria [35]	The venerable "Orange Book" was the standard for several years on how to evaluate the security aspects of a computer system. It was never followed outside the DoD. The word "network" occurs only once in the entire narrative! These are criteria for individual computer systems, before networks became prevalent as they are today!
Common Criteria [30]	Evolution of the "Orange Book", this set of criteria is also to be used across the entire Government before IT systems are security certified. These criteria were developed through international bodies, and cover IT systems across the world.
Joint Vision 2010/2020 [32]	Spells out requirements of "information superiority" needed to win battles of the future. Outlines security in high level terms, nothing specifically on DDoS threats.
National Information Protection Center (FBI) [33]	A division of the FBI that is focused on attacks on US interests that go beyond the criminal. It provides alerts, advisories similar to those provided by CERT ( <a href="http://www.cert.org">www.cert.org</a> ). In addition, NIPC has joined with several private companies to form INFRAGARD.NET ( <a href="http://www.infragard.net">www.infragard.net</a> ), a forum to facilitate information exchange. This is much broader than DDoS, but can encompass it.
Internet 2 & IPV6 [31]	Internet2 is a major new initiative to "upgrade" the Internet infrastructure. IPV6 is the new version of the Internet Protocol (which is generally IPV4). IPV6 eliminates several important security vulnerabilities. DDoS is not one of them, alas. Elimination of "source spoofing" in IPV6 will help somewhat, but adoption will never be 100% for the foreseeable future.
GovNET [32]	This is the pet project of Richard Clarke, the administration's "Cybersecurity Czar". Reactions have been mixed to the idea of creating a completely separate Government infrastructure to support its functions, and it is fair to say that this initiative is currently stalled
Critical Infrastructure Protection Board [34]; See its latest draft "National Strategy to Defend Cyberspace" [36]	Established through an executive order in October 2001, this organization coordinates information security initiatives that involve forming links between various segments of private industry, State and local governments, and Federal agencies. They want problems like DDoS to be solved through partnerships with private industry.

**Figure 1: Existing Initiative & the DDoS Threat**

## **Section 3: Challenges of Building A DDoS Defense**

DDoS flood attacks are difficult to defend against for a variety of technical reasons. To get a good understanding, however, one can avoid the more arcane details of the Internet protocols (which make it particularly convenient to mount such attacks!) and focus upon the most important points.

### **3.1. The Need for Cooperation from “Upstream” Providers**

A DDoS attack manifests itself at a particular enterprise. Once the attack starts, one can usually and quite easily observe computing resources being overwhelmed or servers crashing. One might also get calls from legitimate customers complaining that they cannot get through to your network or website. In fact, with most attacks targeting a corporate network, users inside might also find it hard to communicate with the outside or between one another.

The minimal response of any DDoS defense must be to detect and block the attack. This is not all that easy in the first place, but it will at least protect the internal resources of the enterprise from being damaged. However, this does not solve the problem of allowing legitimate customers to use the network resources. Even if the attack is blocked at the edge of the enterprise network, congestion upstream from the enterprise (i.e., in the carrier space) blocks customers from getting to your network resources. Therefore, the DDoS problem does not lend itself to what are called “point solutions”. A very different approach is needed.

The really difficult DDoS defense problem is that of allowing a way for legitimate customers to get to the enterprise while keeping out attackers. Unfortunately, this is not a problem that one can solve at the enterprise that is feeling the impact of the attack. What is needed is some cooperation from the ISPs that are (usually unwittingly) forwarding the attack traffic to the enterprise. By contacting the ISPs, one can usually get them (eventually) to filter out the traffic that is undesired, thereby making more bandwidth available for normal users. This is not extremely inefficient as a process.

A traditional security problem (e.g., preventing hacking or break-ins) is generally considered the responsibility of the organization that feels the pinch of that particular problem. Unfortunately, DDoS has the peculiar feature that the enterprise under attack *cannot* solve the problem unilaterally, even if it wants to and is willing to expend vast resources on the solution. This has some profound impact on the kinds of technologies that one needs to deal with the problem.

### **3.2. Vulnerabilities of the Internet Infrastructure**

Earlier, we mentioned filtering DDoS attack traffic at the ISP to save upstream bandwidth for regular customers. Figuring out the exact filter to be used at the ISP to eliminate the attack traffic is not easy. One factor is that a typical DDoS attack comes from several locations. A second factor is that, with the present-day Internet, attackers

are able to falsify the source addresses of the attack packets to make it look like they originate from a different location than their true origins – a phenomenon called “source spoofing”. There is nothing inherent in the Internet protocols that prevents this from occurring, and attackers take advantage of this vulnerability to make detection and defense much harder.

Other protocols, such as TCP (Transmission Control Protocol, which are the foundation for much of what we know today as Internet services, also have vulnerabilities. For example, TCP has a simple “hand-shake” protocol to establish connections between programs that wish to communicate over the Internet. Attackers find it easy to send packets that are essentially fake requests simulating parts of the handshake process just to use up valuable computing resources.

In addition, the Internet protocols were designed to be elegant and simple – but with well-behaved programs in mind. For example, after 2 programs have established a connection to communicate using TCP, when one program senses that it is sending traffic too fast for the other program to handle, it slows down, and tries sending traffic at slower rates. This is perfect for the DDoS attacker – by flooding the victim, he can get real customers’ TCP-based programs to slow down even further as they sense network congestion, thereby making his attack even more successful!

### **3.3. Economics of the Internet**

Problems are generally solved quickly when there are economic incentives for people to solve them. As the Internet business has evolved, however, some critical security problems (such as DDoS), have become difficult to solve because none of the major corporate entities responsible for what we think of as the Internet have any reason to solve the problem. In fact, with things the way they are, their rewards lie with the perpetuation of the *status quo*.

As an example, consider large-scale ISPs, managed service providers, or even router companies. These are the entities that are ideally situated to solve the DDoS problem as we have earlier shown, and some of them even have the means (through several emerging technologies) to resolve the problem. However, there is no reason for them to embark on the path of acting to resolve the DDoS problem.

Most Internet infrastructure companies profit from making bandwidth into a commodity. They charge customers for making bandwidth and throughput available to the customer, whether or not the traffic directed to the customer is actually useful to the customer! If there is a threat, such as DDoS, these entities would prefer that customers get even more capacity to guard themselves (which adds to their bottom-line) rather than something that truly distinguishes useful from non-useful traffic (which could, potentially, lower their bottom-line).

## **Section 4: How to Build a DDoS-Resistant Government Infrastructure**

One of the central premises of this White Paper is that it is important (and feasible!) to make the infrastructure inherently ***resistant*** to DDoS attacks. This approach has a

potentially deterrent impact on attackers (their rewards will never match their efforts) and is far superior to the prevalent security paradigm of merely *reacting* to the DDoS attack after it has taken place with defenses.

The Government is a very large (if not the largest) customer for communication and computer equipment and has the clout necessary with the Internet infrastructure companies to break through the socio-economic logjam of enterprises described in Section 4. What is needed is the appropriate set of technologies. **Cs3** has such technologies, and with the cooperation of the Government and one or two major infrastructure companies, a DDoS-resistant Government network is indeed achievable.

**Cs3's MANAnet™** Shield incorporates the critical building blocks for a DDoS-resistant Government infrastructure. Some of the important ideas in *MANAnet* technology include:

- **Elimination of Source Spoofing through Cooperative Neighborhoods of MANAnet's "Fair Service" Routers:** DDoS attacks are made difficult to defend against because of ability of attackers to fake or "spoof" the source addresses on Internet packets. The routers in the cooperative neighborhood are willing to mark packets with accurate path information so that one does not have to rely on data that the attacker controls. Fair service routers take advantage of path data in deciding how traffic should be forwarded. This automatically solves the key problem in DDoS defense: allowing customers a good chance to maintain viable communication even in the presence of DDoS floods. Making very fast "fair service" routers (that can keep up with wire speeds even close to the core of the Internet) will require a 3-way relationship between the Government, a router vendor, and **Cs3**.
- **The Role of Each "Enterprise": Cs3** also provides devices that sit at the edge of the enterprise network – smaller subnetworks of the Government infrastructure. These devices essentially detect DDoS floods directed towards or from a network, and take defensive responses both by themselves and in cooperation with their surrounding "fair service" neighborhoods. The devices are essentially extensions of firewalls. Using patent-pending technology, **Cs3's MANAnet** Firewall detects floods using thresholds of "unexpected" packets (those that are not replies to earlier packets in the other direction). Once an attack is detected, two responses are taken:
  - a) The *MANAnet* Firewall limits the rate of "unexpected" packets that it will forward, thereby throttling all DDoS floods regardless of the mechanism by which they are launched.
  - b) The *MANAnet* Firewall is able to use the path data from cooperative, upstream, *MANAnet* routers to figure out where the attack is coming from using path data that the attacker does not control. The *MANAnet* Firewall communicates with upstream *MANAnet* routers to limit the rate of traffic from the attack paths, thereby pushing the attack even closer to the attacker's infrastructure, allowing more bandwidth for real customers.

- **Incoming and Outgoing Attacks:** Cs3's *MANAnet* technology works to defend against both incoming and outgoing DDoS attacks. In other words, not only can the Government assets be protected from external threats, but the amount of damage that can be done by disgruntled insiders or compromised computers is severely limited.

Some of the competitive benefits of Cs3's *MANAnet* technology include:

1. **Superior Detection Capabilities:** Most DDoS tools in the marketplace use one or both of the following approaches:
  - a) **Signature analysis:** This is rather like virus protection software. A database of known patterns of attack traffic or code that can produce attack traffic is maintained. This works for known attacks, and not for new attacks. One needs to keep the database up-to-date constantly to be even close to effective.
  - b) **Anomaly analysis:** In this approach the system maintains a profile of "normal" traffic or behavior, and deviations from the norm are detected as attacks. The problem is that attackers can get around the defense by adhering to the "normal" profile. Also, such approaches tend to yield unacceptable rates of "false positives", whereby deviations from the normal by non-attackers is detected as an attack, sometimes making the tools unusable in practice.

Cs3's approach is fundamentally better than either of these because it focuses upon the simple fact that DDoS floods can be effective only by sending very high rates of "unexpected" packets. It detects the bad behavior associated with ANY flood attack rather than the attack signature or deviations from normal behavior.

2. **Better Defense:** Cs3's "fair service" router neighborhoods provide the ability for many customers on non-attacking paths to communicate with the victim during the DDoS attack. As we have said, this is the key problem in DDoS defense – to prevent attackers from denying service to good customers. Moreover, Cs3 technology actually *resists* DDoS attacks by mitigating them even before they get to the victim. Such an approach can actually deter flood attacks in the long run, a unique characteristic in the marketplace of DDoS technologies.
3. **Fastest Customer ROI:** Cs3's pricing strategy is very different from that of the competitors. Cs3 devices start at around a few thousand dollars, and are intended to provide the most affordable DDoS protection with the highest level of technical sophistication. In addition, Cs3's technology can be easily incorporated into routers and firewalls with the help of the Government. In this case, there will be an incremental charge added to the price of the devices. In the long run, this will be the best solution, not only for the Government networks, but for all networks.

**Cs3** wishes to work with the owners and operators of large-scale networks to convert to “fair service” infrastructure. In partnership with you, we can build a Government infrastructure that eliminates the vulnerability to DDoS flood attacks.

## **Section 5: References**

- [ 1] Robert Lemos, CNET news.com, June 1, 2001, “DoS Attacks Underscore Net’s Vulnerability”, [http://news.cnet.com/news/0-1003-200-6158264.html?tag=mn\\_hd](http://news.cnet.com/news/0-1003-200-6158264.html?tag=mn_hd)
- [2] Margaret Jane Radin et al, Mazu Networks, “Distributed Denial of Service Attacks: Who Pays?” <http://www.mazunetworks.com/radin-es.html>
- [3] SANS Institute Resources, Intrusion Detection FAQ, Version 1.52, [http://www.sans.org/newlook/resources/IDFAQ/ID\\_FAQ.htm](http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm)
- [4] Kevin Houle & George Weaver, CERT Coordination Center, October 2001, “Trends in Denial of Service Technology”, [http://www.cert.org/archive/pdf/DOS\\_trends.pdf](http://www.cert.org/archive/pdf/DOS_trends.pdf)
- [5] Marc Myers, Client/Server Connection, Ltd, “Securing Against Distributed Denial of Service Attacks”, <http://www.cscl.com/techsupp/techdocs/ddossamp.html>
- [6] Brooke Paul, Network Computing, Jan 1, 2001, “DDOS: Internet Weapons of Mass Destruction”, <http://www.networkcomputing.com/1201/1201f1c2.html>
- [7] Shon Harris, Internet Security, September 2001, “Denying Denial of Service”, <http://www.infosecuritymag.com/articles/september01/cover.shtml>
- [8] Abe Singer, San Diego Supercomputer Center, “Eight Things that ISPs and Network Managers can Do to Help Mitigate DDOS Attacks”, <http://security.sdsc.edu/publications/ddos.shtml>
- [9] Yankee Group News Releases, February 10, 2000, <http://www.yankeegroup.com/webfolder/yq21a.nsf/press/384D3C49772576EF85256881007DC0EE?OpenDocument>
- [10] Sans Newsbytes, Volume 4, Jan 7<sup>th</sup> <http://www.sans.org/newlook/digests/newsbites/0107bonus.txt>
- [11] Bernhard Warner, “Hacker Attacks Shut Down British ISP CloudNine”, February 1, 2002, CNET, <http://news.cnet.com/investor/news/newsitem/0-9900-1028-8672877-0.html>
- [12] 4000 attacks a week <http://www.caida.org/outreach/papers/2001/BackScatter/>
- [13] Government vulnerabilities <http://www.newsbytes.com/news/01/170554.html>
- [14] Terrorist cyber attack warnings from NIPC expert Vatis, <http://www.govexec.com/dailyfed/0901/092601td1.htm>
- [15] Business Software Alliance’s Cyber Security Survey, [www.bsa.org](http://www.bsa.org)

- [16] Howard Schmidt's remarks, washingtonpost.com, June 19, 2002, Interview with Brian Krebs
- [17] National Strategy to Defend cyberspace, <http://www.gcn.com/cybersecurity>
- [18] Internet Security Systems, Denial of Service FAQ Site, <http://www.iss.net/news/denialfaq.php>
- [19] mstream DDoS Attack Tool, David Dittrich, <http://staff.washington.edu/dittrich/misc/mstream.analysis.txt>
- [20] Stacheldraht DDoS Attack, David Dittrich, <http://staff.washington.edu/dittrich/misc/stacheldraht.analysis.txt>
- [21] Tribe Flood Network DDoS Attack, David Dittrich, <http://staff.washington.edu/dittrich/misc/tfn.analysis.txt>
- [22] Trinoo DDoS Attack, David Dittrich, <http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt>
- [23] Steve Gibson, "The Strange Tale of the Denial of Service Attacks Against GRC.com", <http://grc.com/dos/grcdos.htm>
- [24] "Cloud Nine goes away, blames Denial of Service Attacks", Tim Richardson, The Register, <http://www.theregister.co.uk/content/6/23770.html>
- [25] "CERT Hit by DoS Attack", Rutrell Yassin, Internetweek.com, <http://www.internetweek.com/story/INW20010523S0006>
- [26] "Computer Vandals Clog Anti-Vandalism Site", John Schwartz, New York Times, <http://www.acm.org/technews/articles/2001-3/0525f.html#item3>
- [27] "Denial of Service Warning Issued by FBI", CNN.com, <http://www.cnn.com/2001/TECH/internet/05/08/dos.warning.idg/>
- [28] "Information Security: Mid Year 2002 Update", Network World, [http://www.securitytechnet.com/resource/security/consulting/SecuritySR\\_0602.pdf](http://www.securitytechnet.com/resource/security/consulting/SecuritySR_0602.pdf)
- [29] Briefing by Colonel Timothy Gibson of Joint Task Force/Network Operations on a DDoS attack on April 8, 2001 at DARPA Fault Tolerant Networks program PI meeting
- [30] Common Criteria Security Assurance Requirements, <http://www.commoncriteria.org/docs/sar.html>
- [31] Internet2 and IPV6, <http://www.internet2.edu/ipv6/wg-ipv6-charter.shtml>
- [32] Joint Vision 2020, Department of Defense publication, <http://www.dtic.mil/jv2020/jv2020.doc>
- [33] National Information Protection Center, Part of the FBI devoted to the investigation of attacks on US interests that go beyond cyber crimes. <http://www.nipc.gov>
- [34] Critical Infrastructure Protection Board, President's organization to coordinate efforts in infrastructure protection, <http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html>

[35] Department of Defense Trusted Computer System Evaluation Criteria, (Orange Book), <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html>

[36] "National Strategy to Defend Cyberspace : Request for Comment", President's Critical Infrastructure Protection Board, <http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf>

## **Section 6: Appendix: Resources for Government Network Administrators**

The following are an excellent set of resources that will help you to learn more about the DDoS threat and how you and your network can cope with the threat:

1. CERT ([www.cert.org](http://www.cert.org)) is the definitive network security site. Operated by funds from the US Government and administered by Carnegie-Mellon University, they provide excellent and sober expertise on DDoS. Several White Papers that are available here will get you additional details on different kinds of DDoS (and other) threats.
2. SANS Institute "incidents.org" ([www.incidents.org](http://www.incidents.org)) provides alerts and reports on DDoS and security-related incidents. SANS Institute is a good source for training on IT security-related matters as well.
3. National Information Protection Center ([www.nipc.gov](http://www.nipc.gov)) is operated by the FBI. It is another clearinghouse for information on security problems related specifically to US assets that go beyond "normal" computer crimes.
4. DDOSWorld ([www.ddosworld.com](http://www.ddosworld.com)) : a website devoted just to DDoS attacks, assessments of threats, best practices, white papers, and technologies. It is a one-stop shop for those interested in DDoS. It is sponsored by **Cs3**.
5. David Dittrich's Website (<http://staff.washington.edu/dittrich/misc/ddos/>) : provides an excellent collection of articles. The material is slightly more academic than at other sites. David has done the definitive analysis on many specific DDoS attack scripts. You can also find pointers to many other articles from this page.
6. Abe Singer's common-sense suggestions for all network operators to follow regardless of whether they use technological defenses against DDoS (<http://security.sdsc.edu/publications/ddos.shtml>)
7. Internet Security Systems (ISS) provides a good overview of the DDoS problem and how you can deal with it in your infrastructure (<http://www.iss.net/news/denialfaq.php> )
8. Who's Who in Washington on security matters:  
(<http://www.washingtonpost.com/wp-dyn/articles/A50625-2002Jun26.html>)