

POLICY *Review*

DECEMBER 2008 & JANUARY 2009, No. 152

eWMDs

By JOHN J. KELLY III AND
LAURI ALMANN

Policy Review is a publication of the Hoover Institution, Stanford University. Copyright 2008 by the Board of the Trustees of the Leland Stanford Junior University. All rights reserved. Permission is granted to reprint up to 50 copies for classroom or nonprofit use. For other reprint permission, contact *Policy Review*, Reprints Department, 21 Dupont Circle NW, Suite 310, Washington DC 20036 or by email pol-rev@hoover.stanford.edu.

eWMDs

By JOHN J. KELLY III AND
LAURI ALMANN

THE INTERNET HAS enabled the bountiful benefits of eCommerce, and the incorporation of eCommerce into our economies has, in turn, created a dependence on the Internet, similar to our dependence on water, electric, and telephone utilities. Unlike other utilities, however, communication utilities can be crippled without even necessarily being physically attacked — they can be attacked in cyberspace. Such a cyber attack can result in loss of life, loss of wealth, and serious impediments to the flow of goods and services. In a modern just-in-time economy, these disruptions have the potential to cause catastrophic damage. Cyber attacks present a grave new security vulnerability for all nations and must be urgently addressed.

Cyber warfare is asymmetric warfare; more is at risk for us than for most of our potential adversaries. Another asymmetric aspect is that the victims of cyber warfare may never be able to determine the identity of their actual attacker. Thus, America cannot meet this threat by relying solely upon a strategy of retaliation, or even offensive operations in general.

Cyber attacks are best accomplished through exploiting intelligence on the enemy's networks and servers, and on those servers' software, the current vulnerabilities of the software's applications, and standard security practices and typical lapses. Cyber attackers can exploit their targets' networks and servers such that those systems not only stop supporting their intended purposes, but actually work *against* those purposes. As evidenced by recent attacks on the Pentagon computer system, the United States must assume that our potential adversaries in the world are preparing for such attacks.

John J. Kelly III is president of Model Software Corporation. Lauri Almann was permanent undersecretary of defense for the Republic of Estonia from 2004 to 2008.

Cyber warriors may choose to be discreet about high-value targets, the security of which is compromised, and wait for the optimal moment to launch their attacks. But they can also put low-value, low-security targets to coldly efficient use. A low-value target computer can be unwillingly, unknowingly conscripted (by being infected by a virus, worm, or Trojan software) in future attacks as a zombie in a botnet. Botnet is a term for a collection of software robots (bots) which run autonomously on compromised computers (zombie computers). These computers run malicious programs under the command of a so-called bot herder, who can control the group remotely. Any computer can be infected and available for use as part of a botnet without the computer's owner knowing it. In the spring of 2007, Estonia was the victim of a month-long cyber attack, which, according to the *New York Times*, "came close to shutting down the country's digital infrastructure." *Your* personal computer may have been used in that attack without your knowledge. Cyber attacks involve not just one malicious computer but thousands of computers at a time, with new ones constantly joining the fray. Because so many computers are engaged, cyber sallies are all the more difficult to deflect.

When one computer floods a target's server, router, or Internet connection with traffic (i.e., saturating the target with external communication requests, thereby overloading its capacity and effectively making it unavailable for others), it is called a DOS (denial-of-service) attack. A DOS attack is defeated by reconfiguring routers to reject all traffic from the originating IP address — that is, from the address of the aggressor computer. If a large number of computers are used in the battle, though, it is called a DDoS (distributed denial-of-service) attack. In these cases, the routers of the target must be reconfigured to reject the IP address of *each* offensive, zombie computer as it is discovered. DDoS attacks can be overwhelming — it was a DDoS fusillade that crippled Estonia — so all computer owners have a civic duty to secure their machines against becoming part of a botnet.

The U.S. government has a similar duty, but on a larger scale. Because botnets represent such a real threat to our domestic cyberspace and all the assets that those Internet-accessible computers control, it is a vital national interest to secure the domestic Internet.

Attack on Estonia

AMERICA SHOULD LEARN from Estonia's experience. The attacks against that small nation can be divided into several stages.¹ In the first phase, which started on the evening of April 27, 2007, botnets were actually not used. Instead, the so-called ping flooding (simple

¹ Swedish Emergency Management Agency, *Large Scale Internet Attacks. The Internet Attacks on Estonia. Sweden's Emergency Preparedness for Internet Attacks* (2008).

Dos attacks) of several Estonian web sites occurred. These ping attacks were carried out by “hacktivists” incited by several Russian web sites and equipped by these sites with ping-flooding scripts. This initial attack was ostensibly a first phase of a response to the relocation of a Soviet war monument from the center of the Estonian capital-city, Tallinn, to a location at an Estonian military cemetery. The purpose of the initial hacktivist phase apparently was as PR cover for the later botnet phase. It was successful in that regard. It took some time for the international media to realize that the actual nature of the attack was the ensuing more sophisticated, organized, and devastating botnet attack.

Because the hacktivist attacks did not have the desired effect, due to the rapid implementation of filtering and other protective measures, the aggressors escalated the battle. At 11 p.m. on May 8, 2007 (0 hours, May 9, Moscow time), they began employing vast botnets in their attacks. The peak attack is now believed to have been carried out by several different botnets totaling over a million computers located in about 100 different countries. Once the European Union Computer Emergency Readiness Teams (CERTS) were engaged, the attacks originating within Europe effectively ceased. The attacks did continue from other countries, however, thus underscoring the importance of international cooperation in defending against cyber warfare.

The main DDOS attack lasted ten days, from May 8 to May 18. During the period between May 10 and May 15, Estonia’s banks came under fire from the cyber warriors; two major banks had to stop their online services. Ninety-four percent of banking transactions in Estonia are conducted online, and so the attacks had a crippling effect on financial dealings in the country. Most Estonians do not have checkbooks. When the banking system was set up after the nation regained independence in 1991, the decision was made to skip the issuance of checkbooks in favor of direct, online banking. This, of course, made Estonia even more vulnerable to damage from attacks.

Of course, a DDOS attack against online banking lasting several days is enough time to do a great deal of damage to an economy. The attack was not continuous, but came in waves, suggesting that it was not a riot of hackers, but a well coordinated attack. It appears from the pattern of attack that one bot herder was controlling the intensity of the attacks. This demonstrates clearly that there was a single point of control. It is important to note that when the attack began, Estonia had no way of knowing how long the attack would last or whether it would be ongoing.

If the bot herder had been more sophisticated — by spoofing (masquerading as another) originating IP addresses, by better concealing his own location, by enlarging the botnet — then the assault on Estonia could have been far more debilitating and effectively endless (most of the botnet could have been employed to continuously enlarge itself). The commercial router management tools that Estonia used to block the DDOS traffic rendered incoming DDOS traffic eight times less heavy than it would otherwise have been. If the botnet had been substantially larger, though, the nation’s blocking tools

may have been inadequate. As IP addresses were blocked, new zombies joined the attack. Given the large number of zombies available, the attacker was able to expend thousands of zombies per hour. Also, as zombies in the more cooperative countries were blocked, the origin of the attack shifted to countries that did not have any incident management organization (e.g., CERT), or where these organizations were not effective.

And botnets can be vast. In 2005, Dutch authorities arrested three young men who had set up a botnet consisting of 1.5 million zombies.² In 2007, Vint Cerf, one of the co-developers of TCP/IP, the protocol that underlies the Internet, estimated that as much as one quarter of the Internet could already be in botnets.³ Microsoft, in its current Security Intelligence Report, estimates that 10 percent of Windows computers are infected with malware.⁴ While Estonia's experience has highlighted that there are national interests that have the capability and the intention of using cyber attack, their aggression is not the only type currently active in the world.

The world response

JUST AS THE Internet has enabled eCommerce, it has also enabled cyber crime, cyber terrorism, and cyber warfare. Unfortunately, the international community's response to these dangers has been seriously insufficient. Botnets have the potential to do untold damage, and they should be classified as eWMDs (electronic Weapons of Mass Destruction), a term we have coined. We believe it is appropriate to have a category distinction. WMDs can kill in large numbers and cause great disruption. Computers are not generally configured so that they can cause physical damage to themselves or their surroundings, though there is concern about SCADA systems (Supervisory Control and Data Acquisition) — the computer systems that control utilities and process plants in general. The CIA recently disclosed that electric utilities have been successfully attacked. But even if all software and data are securely backed up, there is still potential for great loss due to an eWMD attack.

It was recently determined that a single personal computer could disrupt cellular communications in a city, and that a medium-sized botnet could disrupt cellular communications in the entire United States.⁵ A network attack

² Gregg Keizer, "Dutch Botnet Suspects Ran 1.5 Million Machines," TechWeb News (October 21, 2005).

³ Tim Weber, "Criminals 'may overwhelm the web,'" BBC News (January 25, 2007).

⁴ Microsoft Security Intelligence Report. (January through June 2008). http://download.microsoft.com/download/b/2/9/b29bee13-ccca-48fo-b4ad-53cf85f325e8/Microsoft_Security_Intelligence_Report_v5.pdf

⁵ William Enck, Thomas LaPorta, Patrick McDaniel, and Patrick Traynor, "Exploiting Open Functionality in SMS-Capable Cellular Networks," presented at the 12th ACM Conference on Computer and Communications Security (November 7-11, 2005).

that denies the use of the networked infrastructure could have catastrophic consequences in a modern economy that has become dependent on that infrastructure (as in the case of the Estonian banking system). Attacks on U.S. governmental computers such as those at the Pentagon illustrate the intent to undermine the country's military defense structure. eWMDs have the potential to be the cyber equivalent of a military blockade. While one hopes eWMDs will never be able to cause the loss of life that other weapons of mass destruction (nuclear, chemical, biological) can cause, they should still be recognized as having the potential to destroy livelihoods or even entire economies, as could have happened to Estonia with a larger and more long-term attack.

Traditionally, government has protected life, liberty, and property. But much of a modern economy's wealth resides elsewhere than in, say, physical assets. In a modern economy, much of the wealth is in equities, far beyond the underlying book values and the physical assets. Today's businesses can be destroyed without damaging any of their physical stock. In an economy where stores are run using electronic inventories with automatic ordering, and factories are run using Manufacturing Resource Planning, a disruption to either system or the means for data communication between the two would disrupt the flow of food and goods. Disruption to electronic banking would disrupt all of the companies that rely on those banks. The efficiencies of just-in-time inventory systems also cause the flow of goods to be more vulnerable to disruption. A disruption to the flow of goods and services could trigger damages that cascade through the economy. International trade also brings the possibility that a firm's market share earned over many years could be quickly lost if its customers decide that it is no longer a reliable supplier. But unlike a military blockade or most WMDs, it does not currently require the resources of a nation-state to have a botnet. We will probably always be vulnerable to some degree of cyber crime, cyber terrorism, and cyber warfare, but the one weapon that can be used by all to create catastrophic damage is the botnet. This further underscores the point that we need to institute better safeguards to reduce the scale of the botnet threat.

Of course, as long as computers are connected to the Internet, cyber attacks will occur. Additionally, computer infrastructure can never be perfectly secured by electronic means. For the foreseeable future, so long as computer software is complex and rapidly evolving, there will be bugs for cyber attackers to exploit. But the degree of vulnerability can be dramatically reduced by securing computers and networks through current best practices. The root of the current vulnerabilities, although technical, is also administrative. Many computers are controlled, or administered, both now and for the foreseeable future, by people who do not possess an adequate

*A personal
computer could
disrupt cellular
communications
in a city, and a
botnet could
do the same to
the entire U.S.*

understanding of the current best practices for security. Ideally, anyone who connects his computer to the Internet should be aware of effective ways to secure the machine, but many are not or do not take action, with the result that many machines have become infected.

Thankfully, though, to a considerable degree user ignorance can be compensated for by automated tools. Update management software, part of the Windows and Linux operating systems and some application software, helps make computers more secure. It is designed to be a convenience for users and should properly be considered to be one of our front lines against a cyber attack (though it is not a complete solution, by any means). The U.S. government (and others, too) might consider working with software manu-

*Microsoft's
current Security
Intelligence
Report
estimates that
10 percent of
Windows
computers are
infected with
malware.*

facturers to further develop the effectiveness of these security systems. Similarly, the personal firewalls that are becoming more common on personal machines could be enhanced to help achieve a higher level of protection. And operating systems and applications using passwords should require that the passwords comply with minimum security standards (e.g., nondictionary words of sufficient length). Finally, an adequate degree of logging could be the default to better secure evidence for an investigation. Operating systems and application software can be configured to automatically keep an abbreviated record of all incoming and outgoing traffic. These and other local records would exist only on the PC and be completely private unless and until the owner of the PC chooses to share the records with law enforcement.

If an operating system has a mechanism to audit/enforce proper security, and evidence of the level of security were somehow available to the ISP, then those computers with better security in place could receive preferential treatment in the event of a cyber attack. The ISPs are also in an advantageous position to perform ingress filtering — that is, to check that the “from” address on all packets corresponds to the computer from which the packets are actually coming. This simple check would do much to defeat spoofing and thereby make it easier to determine the origin of attacks.

Another important practice is regular audits. In the corporate environment, outside vendors often perform port scans and advise companies of their current computer vulnerabilities. Governments could work with the ISPs to institute remote automated audits for subscribers as a standard service. The ISPs are well positioned to monitor their networks for suspicious traffic that would indicate that a computer has become infected, and they could also proactively run scanning software to detect machines that are vulnerable and then coordinate with their clients to correct the vulnerability. Perhaps even more importantly, ISPs should have a specific requirement to

prevent improper use. There is anecdotal evidence that some ISPs knowingly provide IP addresses and bandwidth to spammers because of the premium rates such spammers are willing to pay.

The above-mentioned management and auditing services could be performed by greater coordination of existing programs and services. For instance, so long as a user promptly fixes an identified vulnerability, he could be the only one to see the report. If he does not handle it in a timely manner, a report could be sent to his ISP indicating a security risk on the ISP's network. The ISP could then contact the customer to offer technical assistance. A national authority could set standards and provide support to the ISPs.

Developers release patches for their software when new vulnerabilities are discovered. When much Internet software is designed, security is not a major consideration in its development, so the need for patches is common. The rejoinder to this is simple: Do not patch in security, but design it in. If software is created with attention paid to security features, entire categories of vulnerabilities can be eliminated.

Mass-market software is by definition vulnerable to cyber attacks. First, because the software is readily available through commercial or open-source means, hackers can study copies for vulnerabilities. (Open source may be somewhat more secure because it undergoes more scrutiny, but it is also easier to study.) Second, because many copies will exist on the Internet, it is likely that copies will show up in response to even a modest port scan (usually the first step in an attack is to find programs to exploit on computers within a range of IP addresses of interest). Finally, if the software is mass-market, there are likely to be a sufficient number of instances of the software on the Internet to merit investment in discovering its vulnerabilities and developing ways to exploit those vulnerabilities. Because programs that are not mass-market in their deployment do not meet these criteria, heightened security requirements may not need to apply to software that is developed for limited use.

How to enhance the security of mass-market software? Security standards could be established with software developers being obliged to certify that their mass-market software complies with the generally-accepted security practices. Without knowledge of the internal workings of a software program, Underwriters Laboratories-style third-party testing — i.e., running a test suite against something's external interface — may reveal some bugs and vulnerabilities, but will not be adequate to ensure security. And while it is feasible to inspect the source code to ensure that proper practices are used, doing so becomes highly problematic if it involves an external audit — giving source-code access to someone who is not an employee of the developer.

Some ISPs are said to be providing IP addresses and bandwidth to spammers who are willing to pay.

Such access greatly increases the risk of a company's intellectual property being compromised. And as a practical matter, it can be expensive to understand someone else's source code, particularly if it embodies esoteric technical concepts. External audits would also build potentially significant delays into software's release cycle. For these reasons it makes sense for an industry-standards body to publish the security design requirements for mass-market software and require that software developers file a certification of compliance. Sample code could be provided so that this requirement is not burdensome for small developers.

This certification should be required of all the software that runs on all network devices (e.g., routers and switches). It should also be required of the hardware itself, without which the Internet wouldn't work. One of the big problems here is that a substantial amount of this equipment originates in untrustworthy countries. It is not enough to require that developers certify their software and hardware because certifications outside of trusted countries may be worthless. The presence of all these potentially-compromised network devices remains a massive vulnerability.

In August, as Russian tanks rolled into the nation of Georgia, Georgia's websites were also under assault from Russian cyber attackers. Government websites were knocked offline. The lesson: It is essential that the personnel who control the ISP equipment be trustworthy. Georgia had some of its international Internet connections through Russia but thought it had independent communications, since some of the Internet connections went through Turkey. But the access via the ISPs in Turkey also went down, apparently because the ISPs were controlled by the Russian Business Network.

While improving technical capabilities is central to stopping cyber warfare, there are various other areas of concern that the United States should address. For example, there is a need for legislation that would improve the ability of private parties to track down hackers and discover their true identities. When a server is compromised, it is possible for the administrator to preserve logs which might be helpful in determining the origin of the intrusion. Unfortunately, the hacker often hides behind fraudulent registrations. Because it is difficult and expensive for a private individual or small business to pierce these fraudulent, and often foreign, registrations, it is that much easier for the hackers to proceed unimpeded. While it is important to protect privacy, the anonymity afforded by the Internet has helped increase the number of cyber attacks. Hackers currently can launch assaults with little fear of recourse. That's unfortunate; it should be much easier for victims to track down the identities of those who attacked them. Internet registrars should be required to employ a process that is much more rigorous, and much less susceptible to fraudulent registration. Moreover, a government organization could take on the role of active defense against hackers. With the proper legislation, the widespread hacking of private computers could be greatly reduced.

More than a nuisance

ALSO, IT IS in the national interest to diminish the threat of botnets by undermining their financial sources — spammers. In a recent report, IronPort, the email security unit of Cisco Systems, determined that the infamous Storm botnet, which may involve up to 50 million computers, is controlled by Russians who finance their efforts by supporting spammers who sell pharmaceuticals online.⁶ While some botnets may not be associated with foreign governments and are not imminently a national threat, the tools that they develop will be utilized by terrorists and foreign adversaries. The U.S. government should make it a priority to prosecute spammers who support botnets. Two hundred known major spammers are responsible for 80 percent of the spam on the Internet. While prosecutions do occur, they are infrequent and thus not much of a deterrent to other spammers.

One can hope, though, that the lack of prosecution has been because the U.S. government has been busy building a case against spammers through the recent FBI sting “DarkMarket.” The FBI announced 56 arrests as a consequence of DarkMarket.⁷ Among the recently arrested is the HerbalKing Group, which is believed to be responsible for a third of all spam.⁸ Unfortunately, the amount of spam has not appreciably decreased. It appears that those arrested just passed their botnets on to others. If spamming were explicitly outlawed, then many more spammers could be arrested. If the revenues associated with the spam enterprises were severely curtailed by prosecuting the businesses promoted by the spammers, then there wouldn’t be such a valuable incentive for others to continue the enterprise.

Unfortunately, the spam problem is only likely to get worse. If a spam email is 3 KB in size and each zombie computer has a connection that can transmit 1.5 Mb/ per second (i.e., a broadband connection), then 50 spam emails can be sent per second — 180,000 per hour, or 4.3 million per day. Estimates for the cost of renting zombie computers vary. A few years ago estimates ranged from \$30 to \$200 for sending out 1 million spam. A recent investigation of the Storm botnet estimated that the going rate is \$100 per million spam.⁹ The current Microsoft Security Intelligence Report cites the instance of a botnet herder who charged just \$200 dollars per week

⁶ See “2008 Internet Malware Trends” at <http://www.ironport.com/malwaretrends/>.

⁷ Federal Bureau of Investigation, “FBI Coordinates Global Effort to Nab ‘Dark Market’ Cyber Criminals” (October 16, 2008).

⁸ Asher Moses, “Spam flood goes on despite bust,” *Sydney Morning Herald* (October 20, 2008).

⁹ C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. Spamalytics: An Empirical Analysis of Spam Marketing Conversion. CCS’08, (October 27-31, 2008) ACM 978-1-59593-810-7/08/10.

for 6,000 compromised computers (equivalent to 30 computer-weeks for a dollar) — enough capacity to transmit over 800 million spam emails. The Direct Mailers Association reports that direct mail sales campaigns sent through the postal system typically achieve a response rate of 2.15 percent — so they have to have some validity.¹⁰ The investigation into the Storm botnet determined that the actual response rate is 8 in 100 million for the pharmacy sales — a considerable profit margin if the spam campaign costs are at the low end of the estimates. The costs to society are considerable. If each recipient has just one second of his time wasted on average due to a spam campaign, then every one-million-piece campaign costs 277 hours of society's time. The postal campaign, by contrast, might waste 98 seconds, on average, of your time for every two products or services you actually purchase — a much more tolerable imposition.

As briefly mentioned earlier, there is currently no legislation that specifically outlaws spam. The American CAN-SPAM Act of 2003 made fraudulent registrations — a tool used by many spammers — illegal, but it failed to give a legal definition to spam, perhaps out of a desire not to outlaw commercial bulk mail. Of course, every spam filtering company has been able to develop a working “common law” definition of spam. But it is not enough. The U.S. Congress and the European Union must revisit this issue and pass legislation to outlaw spam. The legal definition should then be adopted in international instruments regulating the trade in services.

Active defense

CYBER DEFENSE IS accomplished through a combination of prevention, detection, response, and prosecution. Governments could undertake to work with ISPs, developers, and the general public to devise and support suitable procedures to minimize the vulnerability to botnet attacks, rapidly detect attacks as they occur, assist ISPs in isolating the malicious machines, and support the end user in both securing the evidence and recovering the machine. Finally, governments should ensure that cyber criminals are prosecuted, regardless of whether they are domestic or working in a cooperative foreign country. Governments should also share information and focus on the foreign threats originating from noncooperative countries.

And governments, especially that of the U.S., must begin to see cyber attacks and cyber warfare and eWMDs as the national security threats they truly are. That means engaging in “active defense” and enlisting national police agencies and even the military in the fight. A cyber attack on a U.S. citizen or company, especially one originating outside the nation's borders,

¹⁰ DMA Releases 5th Annual “Response Rate Trends Report.” Direct Marketing Association. <http://www.the-dma.org/cgi/disppressrelease?article=1008>. (October 2007).

should be viewed as a real and serious incursion, and possibly as the prelude to a more serious attack, as it was in Georgia. In the U.S., 85 percent of all critical infrastructure is in the private sector. It is not enough that private individuals and organizations be able to report a break-in after-the-fact. If someone is trying to break in your front door, you expect the police to come immediately. Similarly, the private sector should be able to report break-in attempts and expect a response.

While local law enforcement has the local relationships, the appropriate capabilities reside at the national level in various law enforcement and military organizations. In order to make these capabilities available at the local level, it appears that a coordinating role is required. In the U.S., the National Guard is charged with a similar role and has been performing it in the war on drugs. The National Guard is probably the best suited because if the cyber attack is an actual military or terrorist attack, then time is of the essence. Because what appears to be a criminal act could evolve into something much worse, it is accordingly desirable to keep the National Guard apprised from the first report. Under this approach, whenever a private sector server is under attack, the owner would send the evidence to their state National Guard, which would then perform an initial assessment as to the attack's nature and specifics, with an initial determination as to whether it is an attack or a criminal act, and refer the matter to the appropriate agency. They would then monitor the situation, coordinate the follow-up, and keep the private individual or organization apprised.

Given the demonstrated willingness of aggressors to employ it — as the Russians did against Estonia and Georgia — and the certainty that it will be used again, by state adversaries and terrorists alike, it is crucial that we begin to treat cyber warfare as we would any other form of warfare. We must remove it from the exclusive domain of intelligence operations and establish a Cyber Warfare Command that includes an offensive capability. The U.S. Air Force has taken steps to do just that, but it has yet to be authorized.

In summary, a carefully orchestrated technical program that defends the domestic computer infrastructure should now be a critical goal for every technically-advanced nation. Action is required:

Individuals and businesses. Everyone who uses the Internet needs to understand that they have a civic duty to take reasonable care that their computers are reasonably secure from attack and infection. Any computers that become infected should be promptly cleaned or disconnected. To the extent feasible, forensic evidence should be made available to law enforcement.

Software Industry. Security should be designed into all mass-market applications and operating systems that are connected to the Internet. Designers should enhance comprehensive update management software and personal firewall software so that all machines attached to the domestic Internet can be quickly patched against new vulnerabilities. Logging soft-

ware should by default preserve evidence that would aid those investigating any cyber attack. Operating systems and application software should require secure passwords and be designed for security and certified as such.

ISPs. ISPs should support their subscribers in detecting vulnerabilities, detecting infections, securing evidence, and repairing the infected machines. ISPs should also be required to perform ingress filtering on their routers to counter IP address spoofing. ISPs who profit from knowingly providing IP addresses and bandwidth to spammers should face sanctions. All ISP equipment and personnel should meet standards of trustworthiness.

Legislative bodies. Legislative bodies should pass laws to hinder fraudulent registrations, and they should explicitly outlaw spam campaigns. Legislation could be designed to draw a line between spammers, as exemplified by those identified in the Spamhaus ROKSO database, and legitimate commercial bulk email that is not so designated. This legislation probably should provide a safe harbor for legitimate businesses performing acceptable commercial correspondence. Guidelines may include how the address was obtained, the manner of targeting, the frequency of sending emails, the anticipated and actual response rates, and the number of emails compared to the size of the company's current customer base. Those convicted of serious repeated abuses of the Internet could be fined, and/or banned from further access.

Executive branch. The executive branch should vigorously pursue and prosecute all spammers, hackers, and botnet perpetrators. It should designate and fund an agency to respond to every reported attack; the National Guard may be the appropriate agency for this role. The Defense Department should be tasked to establish a full military capability in cyber operations, perhaps with the Air Force as the lead service. The FBI should have adequate resources to prosecute all major cyber criminal acts.

These measures, along with an ongoing proactive relationship between government and industry to monitor the evolving cyber-warfare threat, evaluate the effectiveness of the measures to counter the threat, and devise improved safeguards, should greatly reduce the magnitude of and resulting damage from future attacks.